S. HRG. 113–891

TAKING DOWN BOTNETS: PUBLIC AND PRIVATE EFFORTS TO DISRUPT AND DISMANTLE CYBERCRIMINAL NETWORKS

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

JULY 15, 2014

Serial No. J–113–70

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PUBLISHING OFFICE
28–403 PDF WASHINGTON : 2018

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

DIANNE FEINSTEIN, California
CHUCK SCHUMER, New York
DICK DURBIN, Illinois
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
AL FRANKEN, Minnesota
CHRISTOPHER A. COONS, Delaware
RICHARD BLUMENTHAL, Connecticut
MAZIE HIRONO, Hawaii

CHUCK GRASSLEY, Iowa, *Ranking Member*
ORRIN G. HATCH, Utah
JEFF SESSIONS, Alabama
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
MICHAEL S. LEE, Utah
TED CRUZ, Texas
JEFF FLAKE, Arizona

Kristine Lucius, *Chief Counsel and Staff Director*
Kolan Davis, *Republican Chief Counsel and Staff Director*

Subcommittee on Crime and Terrorism

SHELDON WHITEHOUSE, Rhode Island, *Chairman*

DIANNE FEINSTEIN, California
CHUCK SCHUMER, New York
DICK DURBIN, Illinois
AMY KLOBUCHAR, Minnesota

LINDSEY GRAHAM, South Carolina, *Ranking Member*
TED CRUZ, Texas
JEFF SESSIONS, Alabama
MICHAEL S. LEE, Utah

Ayo Griffin, *Democratic Chief Counsel*
David Glaccum, *Republican Chief Counsel*

CONTENTS

JULY 15, 2014, 2:31 P.M.

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS

ANSWERS

[Note: At the time of printing, after several attempts to obtain responses to the written questions, the Committee had not received responses from Richard Boscovich.]

TAKING DOWN BOTNETS: PUBLIC AND PRIVATE EFFORTS TO DISRUPT AND DISMANTLE CYBERCRIMINAL NETWORKS

TUESDAY, JULY 15, 2014

UNITED STATES SENATE,
SUBCOMMITTEE ON CRIME AND TERRORISM,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:31 p.m., in room SD–226, Dirksen Senate Office Building, Hon. Sheldon Whitehouse, Chairman of the Subcommittee, presiding.

Present: Senators Whitehouse, Coons, and Graham.

OPENING STATEMENT OF HON. SHELDON WHITEHOUSE, A U.S. SENATOR FROM THE STATE OF RHODE ISLAND

Chairman WHITEHOUSE. I will call this hearing of the Judiciary Committee's Subcommittee on Crime and Terrorism to order, and I thank everyone for being here. I have the permission of my Ranking Member to get underway. He will be joining us shortly, but allowing for opening statements and so forth, I think it is probably the best way to do this, to simply proceed and get underway.

Today's hearing is entitled, "Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks." We are going to be hearing testimony about these botnets and about the threat that they pose to our economy, to our personal privacy, and to our national security.

A botnet is a simple thing. It is a network of computers connected over the Internet that can be instructed to carry out specific tasks. The problem with botnets is that typically the owners of those computers do not know that they are carrying out those tasks.

Botnets have existed in various forms for well over a decade, and they are now recognized as a weapon of choice for cyber criminals, and it is easy to see why. A botnet can increase the computing resources at a hacker's disposal exponentially, all while helping conceal the hacker's identity. A cyber criminal with access to a large botnet can command a virtual army of millions, most of whom have no idea that they have been conscripted.

Botnets enable criminals to steal individuals' personal and financial information, to plunder bank accounts, to commit identity theft on a massive scale. For years, botnets have sent most of the spam that we all receive. The largest botnets are capable of sending billions of spam messages every day.

Botnets are also used to launch distributed denial-of-service—or DDOS—attacks, which can shut down websites by simply overwhelming them with incoming traffic. This is a constant danger for businesses in every sector of our economy, but we have seen this strategy used against everything from businesses to sovereign nations.

The only limit to the malicious purposes for which botnets can be used is the imagination of the criminal who controls them. And when a hacker runs out of uses for a botnet, he can simply sell it to another criminal organization to use for an entirely new purpose. It presents a virtual infrastructure of crime.

Let us be clear. The threat from botnets is not just a threat to our wallets. Botnets are effective weapons not merely for those who want to steal from us, but also for those who wish to do us far more serious harm. Experts have long feared that the next 9/11 may be a cyber attack. If that is the case, it is likely that a botnet will be involved.

Simply put, botnets threaten the integrity of our computer networks, our personal privacy, and our national security.

In recent years, the Government and the private sector have launched aggressive enforcement actions to disrupt and to disable individual botnets. The techniques used to go after these botnets have been as varied as the botnets themselves. Many of these enforcement actions used the court system to obtain injunctions and restraining orders, utilizing innovative legal theories, combining modern statutory claims under statutes such as the Computer Fraud and Abuse Act with such ancient common law claims as trespass to chattels.

In 2011, the Government obtained for the first time a court order that allowed it to seize control of a botnet using a substitute command and control server. As a result, the FBI launched a successful takedown of the Coreflood botnet, freeing 90 percent of the computers Coreflood had infected in the United States.

Microsoft, working with law enforcement, has obtained several civil restraining orders to disrupt and in some cases take down individual botnets, including the Citadel botnet, which was responsible for stealing hundreds of millions of dollars. And earlier this year, the Justice Department and the FBI, working with the private sector and law enforcement agencies around the world, obtained a restraining order allowing them to take over the Gameover Zeus botnet. This action was particularly challenging because the botnet relied on a decentralized command structure that was designed to thwart efforts to stop it.

Each of our witnesses today has played a role in efforts to stop botnets. I look forward to learning more about these and other enforcement actions and the lessons that we should take away from them. We must recognize that enforcement actions are just one part of the answer, so I am interested in hearing also about how we can better inform computer users of the dangers of botnets and what other hygiene steps we can take to address this threat.

My hope is that this hearing starts a conversation among those dealing day to day with the botnet threat and those of us in Congress who are deeply concerned about that threat. Congress, of course, cannot and should not dictate tactics for fighting botnets. That must be driven by the expertise of those on the front lines of the fight.

But Congress does have an important role to make sure that there is a solid legal foundation for enforcement actions against botnets and clear standards governing when they can occur.

We must also ensure that botnet takedowns and other actions are carried out in a way that protects consumers' privacy, all while recognizing that botnets themselves represent one of the greatest privacy threats that computer users face today. They can actually hack into your computer and look at you through your webcam. And we must make sure that our laws respond to a threat that is constantly evolving and encourage rather than stifle innovation to disrupt cyber criminal networks.

I look forward to starting this conversation today and to continuing it in the months ahead. I thank my distinguished Ranking Member for being such a terrific colleague on these cyber issues. We hope that a good piece of botnet legislation can emerge from our work together.

I thank you all for participating in this hearing and for your efforts to protect Americans from this dangerous threat, and before we hear from our witnesses, I will yield to my distinguished Ranking Member, Senator Lindsey Graham.

OPENING STATEMENT OF HON. LINDSEY GRAHAM, A U.S. SENATOR FROM THE STATE OF SOUTH CAROLINA

Senator GRAHAM. Thank you, Mr. Chairman. I just want to acknowledge your work on this issue and everything related to cyber threats. There is no stronger, clearer voice in the Senate than Sheldon Whitehouse in terms of the threats we face on the criminal front and the terrorist front that come from cyber misdeeds, and Congress is having a difficult time organizing ourselves to combat both threats.

But to make sure that this is not an academic exercise, I guess it was last year—or it might even have been a bit longer, but the Department of Revenue in South Carolina was hacked into by—we do not know all the details, but a criminal enterprise that stole millions of Social Security numbers and information regarding companies' charters, revenue, and that has required the State of South Carolina to purchase protection. I think it was a $35 million per year allocation to protect those who had their Social Security numbers stolen, we believe by a criminal enterprise. So it happened in South Carolina. It can happen to any company, any business, any organization in America, and our laws are not where they should be, so the purpose of this hearing is to gather information and hopefully come out and be a friend of law enforcement.

So, Senator Whitehouse, you deserve a lot of credit in my view about leading the effort in the United States Senate, if not the Congress as a whole, on this issue.

Thank you.

Chairman WHITEHOUSE. I am delighted now to welcome our administration witnesses. Before we do, his timing is perfect. Senator

Chris Coons has joined us and yields on making an opening statement, so let us go ahead to the witnesses.

The first is Leslie Caldwell. She is the head of the Criminal Division at the Department of Justice and was confirmed on May 15, 2014. She oversees nearly 600 attorneys who prosecute Federal criminal cases across the country. She has dedicated most of her professional career to handling Federal criminal cases, previously having served as the Director of the Justice Department's Enron Task Force and as a Federal AUSA in U.S. Attorneys' Offices in both New York and California.

And after her testimony, we will hear from Joseph Demarest, who is the Assistant Director for the FBI's Cyber Division. He joined the FBI as a special agent in 1988 and has held several leadership positions within the Bureau, serving as, for instance, head and Assistant Director of the International Operations Division and as the Assistant Director in charge of the New York Division. He was appointed to his current position in 2012, and I have to say that I have had the chance to work very closely with Mr. Demarest, and I appreciate very much the energy and determination that he has brought to this particular arena of combat against the criminal networks of the world. And I look forward to his testimony.

We begin with Assistant Attorney General Caldwell.

STATEMENT OF HON. LESLIE R. CALDWELL, ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Ms. CALDWELL. Thank you, Chairman Whitehouse, Ranking Member Graham, and Senator Coons. Thank you for the opportunity to discuss today the Justice Department's fight against botnets, and I particularly want to thank the Chair for holding this hearing and for his continued leadership on these important issues.

The threat from botnets—defined in simple terms as networks of hijacked computers surreptitiously infected with malicious software, or malware, which are controlled by an individual or an organized group for criminal purposes, has increased dramatically over the past several years. Criminals are using state-of-the-art techniques, seemingly drawn from science fiction movies, to take control of thousands or even hundreds of thousands of victim computers, or bots. They can then command these bots to do various things, as Senator Whitehouse indicated. They can flood an Internet site with junk data. They can knock it offline by doing that. They can steal banking credentials, credit card numbers, other personal information, other financial information; send fraudulent spam email; or even spy on unsuspecting computer users through their webcams.

Botnet attacks are intended to undermine Americans' privacy and security and to steal from unsuspecting victims. If left unchecked, they will succeed in doing so. As cyber criminals have become more sophisticated in recent years, the Department of Justice, working through highly trained prosecutors at the Computer Crime and Intellectual Property Section of the Criminal Division, which I will call "CCIPS," the National Security Division of the Justice Department, U.S. Attorneys' Offices across the country, and the FBI and other law enforcement agencies, we have likewise adapted and advanced our tactics to meet this threat.

As just one example, in May of this year, CCIPS, the U.S. Attorney for the Western District of Pennsylvania, and the FBI, in partnership with other Federal and private sector organizations, disrupted the Gameover Zeus botnet and indicted a key member of that group that operated that botnet. Until its disruption, Gameover Zeus was widely regarded as the most sophisticated criminal botnet in existence worldwide. From 2011 through 2014, Gameover Zeus infected between 500,000 and 1 million computers, and it caused more than $100 million in financial loss.

Put simply, the botmaster stole personal information from victim computers and with the click of a mouse, used that stolen information to empty bank accounts and rob small businesses, hospitals, and other victims by transferring funds from the victims' accounts to the criminals' own accounts.

They also used Gameover Zeus to install CryptoLocker, which is a type of malware known as "ransomware." That was installed on infected computers, and CryptoLocker enabled these criminals to encrypt key files on the infected computers and to charge victims a ransom for the release of their own files. In the short period between its emergence and our action, CryptoLocker infected more than 260,000 computers worldwide.

The Department's operation against Gameover Zeus began with a complex international investigation conducted in close partnership with the private sector. It continued through the Department's use of a combination of a court-authorized criminal and civil legal process to stop infected computers from communicating with one another and with other servers around the world. The investigation and operation ultimately permitted the team not only to identify and charge one of the leading perpetrators, but also to cripple the botnet and to stop the ransomware from functioning.

Moreover, the FBI was able to identify victims and, working with the Department of Homeland Security, foreign governments, and private sector partners, was able to facilitate the removal of malware from many victim computers. As we informed the court last week, at present the Gameover Zeus botnet remains inoperable and out of the criminals' hands. Gameover Zeus infections are down 30 percent, and CryptoLocker remains non-operational.

As the successful operation demonstrates, we are employing investigative and remedial tools that Congress has given us to protect our citizens and businesses. We have leveraged our strengths by partnering with agencies all over the world and in the private sector. If we want to remain effective in protecting our citizens and businesses, however, our laws and resources must keep pace with the increasingly sophisticated tactics and growing numbers of our adversaries. Our adversaries are always adapting. So must we.

In my written statement, I describe several legislative proposals and resource increases that will assist the Department in its efforts to counter this threat. These proposals include an amendment to the Computer Fraud and Abuse Act and several other proposals. We very much look forward to working with the Committee to address these issues. We also need additional resources at the Department to continue to disrupt botnets, including hiring new attorneys, as indicated in my statement.

Thank you again for the opportunity to discuss our work in this area, and I look forward to answering any questions you might have.

[The prepared statement of Ms. Caldwell appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you, Assistant Attorney General Caldwell.

And now, Mr. Demarest, Director Demarest.

STATEMENT OF JOSEPH DEMAREST, JR., ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION, WASHINGTON, DC

Mr. DEMAREST. Good afternoon, Chairman Whitehouse, Ranking Member Senator Graham, and Senator Coons. Thank you for holding this hearing, Chairman Whitehouse, and I look forward to discussing the progress the FBI has made on campaigns to disrupt and disable our significant botnets that you know that we target.

Cyber criminal threats pose very real risks to the economic security and private sector of the United States and its citizens. The use of botnets is on the rise. Industry experts estimate that botnet attacks have resulted in the overall loss of millions of dollars from financial institutions and other major businesses. They also affect universities, hospitals, defense contractors, government, and even private citizens.

The "weapons" of a cyber criminal are tools, like botnets, which are created with malicious software that is readily available for purchase on the Internet. Criminals distribute this malicious software, also known as 'malware,' that can turn a computer into a bot. When this occurs, a computer can perform automated tasks over the Internet, without any direction from its rightful user. A network of these infected computers is called a "botnet," as you pointed out. Botnets can be used for organized criminal activity, covert intelligence collection, or even attacks on critical infrastructure.

The impact of this global cyber threat has been significant. According to industry estimates, botnets have caused over $9 billion in losses to U.S. victims and over $110 billion in losses globally. Approximately 500 million computers are infected each year, translating into 18 victims per second.

The FBI, with its law enforcement partners and private sector partners, to include the panel of distinguished presenters today from Microsoft, Symantec, and Farsight, has had success in taking down a number of large botnets. But our work is never done, and by combining the resources of Government and the private sector, and with the support of the public, we will continue to improve cybersecurity by identifying and catching those who threaten it.

Due to the complicated nature of today's cyber threat, the FBI has developed a strategy to systematically identify cyber criminal enterprises and individuals involved in the development, distribution, facilitation, and support of complex criminal schemes impacting U.S. systems. The complete strategy involves a holistic look at the entire cyber underground ecosystem and all facilitators of a computer intrusion.

The FBI has initiated an aggressive approach to disrupt and dismantle most significant botnets threatening the U.S. economy and our national security. The initiative, coined "Operation Clean Slate," is spearheaded by the FBI, our National Cyber Investigative Joint Task Force, along with a host of USG partners to include DHS and the private sector. It is a comprehensive, public-private effort engineered to eliminate the most significant botnets jeopardizing U.S. interests by targeting the bot infrastructure and at the same time the coders or those who are responsible for creating them. This initiative incorporates all facets of the USG, as I mentioned, international partners, major ISPs, the U.S. financial sector, and other private sector stakeholders like the many cybersecurity services. Again, I would point out Dell Secure Works being one of the main, and we talked about Gameover Zeus.

Operation Clean Slate has three objectives: to degrade or disrupt the actor's ability to exfiltrate sensitive information from victims; to increase the actor's cost of business; and to seed uncertainty in the actor's cyber activity by causing concern about potential or actual law enforcement action against them.

Just a brief description about some of the successes of late. In December 2012, the FBI disrupted an international organized cybercrime ring related to Butterfly Botnet, which stole computer users' credit card, bank account, and other personally identifiable information. The Butterfly Botnet compromised more than 11 million computer systems and resulted in over $850 million in losses. The FBI, along with international law enforcement partners, executed numerous search warrants, conducted interviews, and arrested 10 individuals from Bosnia and Herzegovina, Croatia, Macedonia, New Zealand, Peru, the United Kingdom, and the United States—all of this not possible without DOJ, CCIPS in particular, and local U.S. Attorneys' Offices.

In June 2013, again, the formal debut of Operation Clean Slate, the team, in coordination with Microsoft and financial service industry leaders, disrupted the Citadel Botnet that you pointed out, which had facilitated unauthorized access to computers of individuals and financial institutions to steal online banking credentials, credit card information, and other PII. Citadel was responsible for the loss of over a half billion dollars. Over 1,000 Citadel domains were seized, accounting for more than 11 million victim computers worldwide.

Building on that success of the disruption of Citadel, in December 2013, the FBI and Europol, together with Microsoft and, again, the Operation Clean Slate team and other industry partners, disrupted the ZeroAccess botnet. ZeroAccess was responsible for infecting more than 2 million computers, specifically targeting search results on Google, Bing, and Yahoo search engines, and is estimated to have cost online advertisers $2.7 million each month.

Again, in April 2014, the Operation Clean Slate team investigative efforts resulted in the indictments of nine alleged members of a wide-ranging racketeering enterprise and conspiracy that infected thousands of business computers with malicious software known as "Zeus" or "Jabba Zeus," which is malware that captured passwords, account numbers, and other information necessary to log into online banking accounts. The conspirators allegedly used the information captured by Zeus to steal millions of dollars from account-holding victims' bank accounts.

Later, in June 2014, yet another operation by the Clean Slate team announced a multinational effort to disrupt the Gameover Zeus botnet, the most sophisticated botnet that the FBI and its allies had ever attempted to disrupt. Gameover Zeus is believed to be responsible for the theft of millions of dollars from businesses and consumers in the U.S. and around the world. This effort to disrupt it involved impressive cooperation with the private sector—namely, Dell Secure Works—and international law enforcement. Gameover Zeus is an extremely sophisticated type of malware designed specifically to steal banking and other credentials from the computers it infects. In the case of Gameover Zeus, its primary purpose is to capture banking credentials from infected computers, then use those credentials to initiate or redirect wire transfers to accounts overseas that are controlled by the criminals. Losses attributable to Gameover Zeus are estimated to be more than $100 million.

Much like the FBI's other investigative priorities and programs, our focus is impacting the leaders of the criminal enterprises and terrorist organizations we pursue. We are focusing the same effort on the major cyber actors behind the botnets. We remain focused on defending the United States against these threats, and we welcome the opportunity like the one today to discuss our efforts.

We are grateful for the Committee's support, and yours in particular, Senator Whitehouse, and we look forward to working closely with you as we continue to forge aggressive campaigns against botnets.

[The prepared statement of Mr. Demarest appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you very much.

Assistant Director Demarest, there have to be, what, hundreds of thousands, millions of botnets out there?

Mr. DEMAREST. Yes.

Chairman WHITEHOUSE. One could say, "So many botnets, so little time." So given that, what are your factors for prioritizing which ones to go after through the Clean Slate program or just generally?

Mr. DEMAREST. So by Operation Clean Slate, it was to forge an alliance with the private sector and Government and then prioritize the most egregious botnets that are out there in the wild that we know about. So working with not only Government, DHS being principal, and friends in the intelligence community, but also I will say in the private sector, Microsoft being chief, and looking across, you know, the world, and those botnets that are seemingly causing the most damage, economic damage or other means or potentially physical damage, and prioritizing those and then developing a campaign about going after not only the infrastructure but the actors behind that botnet or those botnets.

Chairman WHITEHOUSE. Assistant Attorney General Caldwell, one of the—this pre-dates you, but I have had some concerns based on my time in the Department of Justice as a U.S. Attorney about the way in which the Department has responded to the botnet threat. I think you are doing a good job, but there is a cultural divide sometimes between the criminal prosecutors and the civil attorneys for the Government.

These cases that take down the botnet tend to be civil cases in nature, so I have worried a bit about the extent to which it is instinctive on the part of criminal prosecutors to think that that is a lesser task and a lesser pursuit than what they are doing and whether that gets in the way of adequately pursuing the civil remedies that shut these botnets down.

The second is that when the Coreflood takedown took place, it appeared to me that that was kind of an ad hoc group of very talented people who were brought together to address themselves to Coreflood and to succeed at taking it down; but once the operation was complete, they went back to their individual AUSA slots in offices around the country, and the effort was dispersed.

I think that the botnet problem is a continuing one. I think as soon as you strip out, as Mr. Demarest said, some of the worst offenders, others pop up into the next most wanted botnet slot. And I am interested first in how you are making sure that this is prioritized, despite the civil nature of the legal proceeding that cures the botnet problem, that strips it out of the system, and what you have done to try to establish a permanent, lasting institutional presence for taking down botnets without having to reassemble teams each time a botnet rears its head as a target.

Ms. CALDWELL. Thank you, Senator. I think that the Gameover Zeus operation is the perfect example of how we see this going forward. Although I would not dispute that there are some criminal Assistant U.S. Attorneys who may think that the civil Assistant U.S. Attorneys have a less exciting job, we do not see it that way. The civil component, as you indicated, is a very critical part of this, but there are different ways to approach botnets. They are all different, as you indicated earlier.

In Gameover Zeus, we used a combination of civil and criminal authorities, and I think that is—again, it is not one size fits all, but I think that is likely what we will continue to see in the future. As you know, the leading perpetrator of that particular botnet was actually indicted criminally, and the civil injunctions were obtained at the same time. It was very carefully coordinated. There was a lot of communication between the civil prosecutors who were handling the injunction paperwork and the criminal prosecutors who were—it was really all one team. So I think the civil tool is a very important tool, and we expect to continue to use it.

There are some holes in that tool. Right now we are permitted to get a civil injunction against fraud and a civil injunction against wiretapping. But as you indicated in your opening remarks, botnets are not always engaged in fraud and wiretapping. They are engaged in other things, too. So one thing that we would like to see happen is an amendment to the statute to permit injunctions in other circumstances in which we see botnets operating.

Then on the issue of the institutional knowledge, the Computer Crime and Intellectual Property Section is really the receptacle—that is a bad word, but where all that knowledge is based. The Computer Crime and Intellectual Property Section has a headquarters component. It has field components. It has a lot of institutional knowledge about botnets, so that if one prosecutor leaves, the knowledge is not going to leave. We coordinate regularly with the FBI, and there is a lot of coordination. There is a lot of coordination with the Computer Hacking Intellectual Property Network in the U.S. Attorneys' Offices. And there really is an institutional base of knowledge about botnets. So even——

Chairman WHITEHOUSE. In a nutshell, you feel right now that that task has been adequately institutionalized in the Department, that there will be continuity and persistence rather than ad hoc efforts?

Ms. CALDWELL. Yes, and I think that although they were not as prominent, there were at least a half-dozen other botnet takedowns in the last couple of years between Coreflood and Gameover Zeus. So there is definitely—it is definitely a priority, and there is definitely a focus, and there is a lot of knowledge among the CCIPS prosecutors and their counterparts at the FBI about these botnets. And they will keep coming, and we will keep attacking them.

Chairman WHITEHOUSE. I will yield to my Ranking Member, but my impression was that some of those were sort of sporadic and ad hoc takedowns that appeared in individual U.S. Attorneys' Offices and not necessarily consistent with a continuing, lasting, persistent presence stripping down one botnet after another. And I am glad that you have gotten to where you have gotten, so thank you.

Senator Graham.

Senator GRAHAM. Are you the Eliot Ness of botnets?

[Laughter.]

Senator GRAHAM. Do we have an Eliot Ness of botnets?

Ms. CALDWELL. I think he is the Eliot Ness of botnets.

Senator GRAHAM. Okay. Well, no matter what kind of behavior you are dealing with, you try to deter it, make people think, "If I do this, I am going to get caught, and if I get caught, bad things are going to happen." What do you think the deterrence is like right now, Mr. Demarest?

Mr. DEMAREST. Well, I think it is significant now, and in years past, maybe not as much so, where they did travel and they felt they could take some actions with impunity. And we are finding today, based on some of the actions, enforcement actions that were successful, we are causing impact because we actually see that in other collections, them talking amongst each other, and concern about traveling now, which is a way of containing some of the threats that we see in individuals today.

Senator GRAHAM. What nation states do we need to worry about in terms of being involved in this activity?

Mr. DEMAREST. I would say the Nation states of EurAsia, principally. We have seen a lot of the criminal actors coming from that area of the world.

Senator GRAHAM. Okay. Are they reliable partners, the governments?

Mr. DEMAREST. We are opening dialogue, I will say on that front. I think you will find some of our Russian counterparts in law enforcement are a bit more agreeable, but, you know, as in any new relationship, I think especially in this space, we are working toward improving them.

Senator GRAHAM. If it is possible, maybe by the end of the year could you provide the Committee with a list of countries that you think have been good partners and the list of countries you think have been resistant.

Mr. DEMAREST. Yes, easily done, based on our activities or working with the countries we do work with.

Senator GRAHAM. Well, once we identify them, maybe we can change their behavior. There are all kinds of ways of getting people's attention.

Was this a problem 5 years ago? How long ago has this been a problem?

Mr. DEMAREST. This has existed for years, and probably we are just now—you know, this is the tip of the iceberg. And I think as we get more sophisticated internally in the U.S. Government in seeing and being able to identify——

Senator GRAHAM. What made us aware of it today more than, say, 5 years ago? Just the consequences?

Mr. DEMAREST. I think the consequences, I think victim reporting, I think major losses occurring to private industry.

Senator GRAHAM. Is there any end to this? How far can these people go?

Mr. DEMAREST. They will keep on going. As you can see, each bot will evolve. We take actors off. Now they will change. We see a complete evolution. But, again, we are actually placing—at least there is a price to pay for actually engaging in this activity now.

Senator GRAHAM. Are terrorist organizations involved in this?

Mr. DEMAREST. We track them very closely. I would say there is an interest. But much further than that, Senator Graham, probably in a different setting we could give you a further briefing.

Senator GRAHAM. Ms. Caldwell, on the civil-criminal aspect of this, what are the couple things that you would like Congress to do to enhance your ability to protect our Nation? I am sure you have got this written down somewhere, but just for the average person out there listening to this hearing, what are the couple things you would like to see us do?

Ms. CALDWELL. Well, one is the one that I already mentioned, which is changing the civil injunction ability so that we will have the capability to enjoin botnets other than those that are engaged in fraud and wiretapping, because there are, for example, distributed denial-of-service attacks. Right now we cannot get an injunction against that. So we would like to be able to do that.

Senator GRAHAM. Do we need to increase penalties?

Ms. CALDWELL. That is an interesting question, Senator, and I think that we have been seeing increased penalties being imposed by courts. So——

Senator GRAHAM. I mean statutorily, Mr. Demarest, do we need to change any statutes to make this bite more?

Mr. DEMAREST. I will defer to Ms. Caldwell, but—I will defer to you.

Ms. CALDWELL. Yes, I think that the maximum sentences under most of the statutes are adequate. I do not think we need any kind of mandatory minimums because we have been seeing judges imposing sentences around the 7-, 8-, and 9-year range, which is, I think, a very substantial sentence.

There are a couple other things that we would like to see. Right now there is no law that explicitly covers the sale or transfer of a botnet that is already in existence, and we have seen evidence that a lot of folks sell botnets. They rent them out, and we would like to see a law that addresses that.

One other thing which is a little bit off point but I think is still relevant to botnets, is that right now there is no law that prohibits the overseas sale of U.S. credit cards unless there has been some action taken in the United States or unless money is being transferred from overseas to the United States. So we see credit card—situations where people have millions of credit cards from U.S. financial institutions, but they never set foot in the United States. That is currently not covered by our existing law.

Senator GRAHAM. So you could steal my credit card information from overseas and basically be immune.

Ms. CALDWELL. Correct, unless you transferred proceeds of your scheme back to the United States.

Senator GRAHAM. Okay. One last question here. When they basically seize your computer, hijack your computer, the information contained therein, they actually hold—I mean, they make a ransom demand? How does that work?

Ms. CALDWELL. Under CryptoLocker what happened—and I am certainly not a technical expert, so jump in—you would be on your computer, and you would see something flash up on your screen that basically told you all your files were encrypted and would remain encrypted until you paid a ransom. And you had to pay the ransom within X hours, and if you did not pay, your files would all be deleted.

Mr. DEMAREST. In a payment made through Bitcoin or whatever. Whatever the established venue is, they expected payment within a given amount of time, and if not, your box would be encrypted.

Senator GRAHAM. Do people pay?

Mr. DEMAREST. They do.

Senator GRAHAM. What is the biggest payout you have seen?

Mr. DEMAREST. Well, of all CryptoLocker and then Cryptowall now, and where there is a major concern, they have paid probably in excess of $10,000. But they are focused more now on major concerns, businesses, and entities as opposed to single victims.

Senator GRAHAM. Is that extortion under our law?

Ms. CALDWELL. Yes.

Senator GRAHAM. So you do not need to change that statute?

Ms. CALDWELL. No. The problem is, though, as with a lot of these cybercrimes, most of the people who are engaged in this activity are overseas.

Senator GRAHAM. Thank you.

Chairman WHITEHOUSE. Let me recognize Senator Coons, who has been very interested and dedicated to this topic and whose home State is very energized on this topic because the Delaware National Guard actually has a cyber wing that is very active, and they are one of the best cyber National Guard detachments in the country. I say “one of the best” because Rhode Island has one, too.

Senator Coons.

Senator COONS. Thank you very much. Thank you, Chairman Whitehouse, and thank you, Senator Graham. You have both been great and engaged and effective leaders on this issue.

So to the point raised by the Chairman, given the persistency of this threat, given its trajectory, its scope, its scale, and the resources that you are having to deploy in order to take down these botnets and in order to break up the criminal gangs, is it acceptable, is it possible for us to deal with this threat with a Federal law enforcement response alone? Do we need a partnership from State and local law enforcement? I assume the answer is yes. And how are we doing at delivering an integrated capability, Federal, State, and local, first?

Second, what kind of capabilities do businesses and individuals and the private sector and citizens have? And what are we doing to help scale up that? Because the resiliency of our country, our ability to respond to these threats, as we all know, much as it is with natural disasters or with terrorism threats, requires a sort of "everybody engaged" response that engages our private sector, engaged entrepreneurs, and engages State and local as well as Federal law enforcement? So I would be interested in your answer to that question.

Mr. DEMAREST. Sure. Thank you, Senator Coons. So on the State and local question, we have cyber task forces throughout each of our offices. There are 56 out there. Each office is engaging at the local level to bring State and local authorities aboard, whether investigator or net defenders from the organizations they represent. It is very difficult because of resources being somewhat constrained at the State and local level and fully understanding and appreciating what the threat is.

Operation Wellspring is an effort we kicked off, and what that is, it is focused on Internet fraud, whether defrauding the elderly, it is real estate fraud, and working with State and local, having them either bring an officer or investigator aboard, or an analyst. We work closely with them to foster their skills or to develop their skill in this area working cybercrime. It has worked well in some of the initial offices in Salt Lake City, with the Utah Department of Public Safety, and down in Dallas with some of the local departments, the Dallas Police Department. We have got a long way to go in that space and for them to fully appreciate what the threats are today facing the public or the citizens they are responsible for.

In the private sector, we have worked far and wide and somewhat limited in force. We have now focused on those priority sectors, if you will, that are most threatened. But we have found time and time again the most threatened and the most vulnerable are those small to medium-sized business owners where they may have one single person that is responsible for Internet security or cybersecurity, information assurance and the like. So it is not—it is how do we target that band and actually bring them aboard when we are still working through—we actually had health care, representatives from the health care industry in our headquarters working through what that relationship would look like with health care, because we have focused on, as you can imagine, finance, energy, the IT, telecommunications and the like over the past 2 years, and now how do we broaden that effort out?

Senator COONS. Implicitly, from your reference to health care, I share your concern that as we have transitioned to electronic medical records, we now have an online treasure trove of data for cyber criminals to go after?

Ms. Caldwell.

Ms. CALDWELL. Yes, I think any online data base is vulnerable. Some obviously have more security protections than others. And as you indicated, Senator Coons, the health care data bases obviously have a lot of very sensitive personal information. So we have seen, I know, in some of the botnets that we have seen over the years, including, if I am not mistaken, Gameover Zeus, some of the victims were hospitals. So that is a very serious area of concern, which we are very concerned about.

Senator COONS. Let me just ask one other question. As Senator Whitehouse referenced, both of our States are blessed to have network warfare squadrons of the National Guard. The Air National Guard in Delaware has stood up and grown and developed this National Guard capability which takes advantage of the fact that we have a fairly sophisticated financial services community. We have large data centers. We have a lot of credit card processing, and as a result, there is a lot of fairly capable and sophisticated online security and financial services security professionals who can then also serve in a law enforcement and national security, first responder context through the National Guard.

What lessons do you think we could learn from that partnership, that collaboration in our two home States? And how could that lead us to a better scale-up of the needed Federal work force to respond to and deal with these law enforcement challenges?

Mr. DEMAREST. There is a treasure trove of skill in the Guard and Reserve forces. We participated, actually hosted down at the FBI Academy the Cyber Guard exercise in 2014. We brought personnel in from around the field, at least 50 from our local cyber task forces that corresponded with the local Guard units that were in. Great capability there. Our Director, along with the Deputy Director, had a meeting with the combatant command, cyber command, OSD, and joint staff about how we better correlate or collaborate in this space.

Tomorrow we actually have another meeting with the combatant commanders at my level to actually put this in place along with the Reserve and Guard units.

As you know, Admiral Rogers held a meeting at NSA recently to talk through what that looks like in working with cyber command, the Guard forces, and Reserve forces, and what skills they bring, how that may assist the FBI in our operations, and also training opportunities that we can leverage with one another.

Senator COONS. Terrific. Thank you for your testimony. I look forward to hearing more about the development of this partnership.

I just want to thank you for your leadership in this area, Senator Whitehouse.

Chairman WHITEHOUSE. Well, I will let you two go. I am sure we could ask you questions all afternoon. This is such a fascinating and emerging area of criminal law enforcement. I appreciate very, very much the work that you do, and I want you to pass on to Attorney General Holder my congratulations for the dedication that he has brought to this pursuit, particularly as exemplified by the Gameover Zeus takedown and by the indictment of the Chinese

PLA officials. Those were both very welcome steps, and I am looking forward to seeing more criminal prosecution of foreign cyber hackers. I think the opening gambit with the indictment of the Chinese PLA folks was really terrific. So congratulations to you both. Thank you for your good work, and we will release you and call the next panel forward.

Chairman WHITEHOUSE. All right. Thank you all so much for being here. This is a really terrific private sector panel on this issue, and I am grateful that you have all joined. I will make the formal introductions right now of everyone, and then we can just go right across with your statements.

Our first witness is going to be Richard Boscovich, who is the assistant general counsel on Microsoft's Digital Crimes Unit, a position where he developed the legal strategies used in the takedowns and disruptions of several botnets, including the Citadel, Zeus, and Zeus Access botnets. He previously served for over 17 years at the Department of Justice as an Assistant U.S. Attorney in Florida's Southern District, where he directed the district's Computer Hacking and Intellectual Property Unit.

We will next hear from Cheri McGuire, the vice president of global government affairs & cybersecurity policy at Symantec Corporation, which is one of our leading cybersecurity providers in this country. She is responsible for Symantec's global public policy agenda and government engagement strategy, including cybersecurity, data integrity, critical infrastructure protection, and privacy. Before she joined Symantec in 2010, she was director for critical infrastructure and cybersecurity in Microsoft's Trustworthy Computing Group, and before that she served in numerous positions at the Department of Homeland Security, including as Acting Director and Deputy Director of the National Cyber Security Division and the US-CERT.

We will then hear from Dr. Paul Vixie, who is the chief executive officer of Farsight Security, which is a commercial Internet security company. He previously served as the chief technology officer for Abovenet, an Internet service provider, and as the founder and CEO of MAPS, the first anti-spam company, and as the operator of the "F" DNS root name server. Dr. Vixie is the author of several Internet standards related to DNS and was the maintainer of BIND, a popular open-source DNS software system, for 11 years. And he was recently inducted into the Internet Hall of Fame.

Finally, we will hear from Craig Spiezle, who is the executive director, founder, and president of the Online Trust Alliance. The Online Trust Alliance encourages best practices to help protect consumer trust, and he works to protect the vitality and innovation of the Internet. Prior to founding the Online Trust Alliance, he worked at Microsoft, again—the fraternity—where he drove development of anti-spam, anti-phishing, anti-malware, and privacy-enabling technologies. He is on the board of the Identity Theft Council and was appointed to the FCC's Communications Security, Reliability, and Interoperability Council. He is also a member of InfraGard, which is the partnership between the FBI and the private sector.

So these are immensely knowledgeable and experienced witnesses, and let me begin with Richard Boscovich. We are so glad you are here. Thank you.

STATEMENT OF RICHARD BOSCOVICH, ASSISTANT GENERAL COUNSEL, DIGITAL CRIMES UNIT, MICROSOFT CORPORATION, REDMOND, WASHINGTON

Mr. BOSCOVICH. Chairman Whitehouse, Ranking Member Graham, and Members of the Subcommittee, my name is Richard Domingues Boscovich, and I am an assistant general counsel in Microsoft's Digital Crimes Unit. Thank you for the opportunity to discuss Microsoft's approach to fighting and detecting botnets. We also thank you for your leadership in focusing attention to this complicated and important topic.

Botnets are groups of computers remotely controlled by hackers without their owners' knowledge or consent, enabling criminals to steal information and identities, to disrupt the operation of computer networks, and to distribute malicious software and spam. I will describe for you how Microsoft, one, works with partners to fight botnets; two, raises costs for cyber criminals by disrupting their tools; and, three, carefully designs these operations to protect consumers.

To understand the devastating impact of botnets, we can look at how they affected one victim. Consider Eunice Power, a chef in the United Kingdom, who turned on her laptop 1 day to find a warning that she could not access her files unless she paid a ransom to cyber criminals within 72 hours. When she failed to meet the deadline, all of her photos, financial account information, and other data were permanently deleted. All this was caused by a botnet. She later told a reporter, "[i]f someone had robbed my house it would have been easier."

Indeed, botnets conduct the digital equivalent of home invasions, but on a massive scale. Botnet operators quietly hijack webcams to spy on people in their own homes and later sell explicit photographs of the unsuspecting victims on the black market. They use malicious software to log every keystroke that users enter on their computers—including credit card numbers, Social Security numbers, work documents, and personal emails. They send deceptive messages designed to appear as though they were sent by banks that convince people to disclose their financial account information.

Now, Microsoft has long partnered with other companies and global law enforcement agencies to battle malicious cyber criminals such as those who operate botnets. We do not and cannot fight botnets alone. As the title of this hearing suggests, fighting botnets requires efforts from both the private and the public sector. We routinely work with other companies and domestic and international law enforcement agencies to dismantle botnets that have caused billions of dollars in worldwide economic damage. I joined efforts to demonstrate that public-private partnerships are highly effective at combating cybercrime. In reality, problems as complex as botnets cannot be addressed without partnerships.

Microsoft's philosophy to fighting botnets is simple: We aim for their wallets. Cyber criminals operate botnets to make money. We disrupt botnets by undermining cyber criminals' ability to profit from their malicious attacks.

Microsoft draws on our deep technical and legal expertise to develop carefully planned and executed operations that disrupt botnets pursuant to court-approved procedures. In general terms, Microsoft asks a court for permission to sever the command-and-control structures of the most destructive botnets. This breaks the connection between the botnets and the infected computers to control. Traffic generated by infected computers is either disabled or routed to domains controlled by Microsoft where the IP addresses of the victims can be identified.

Now, privacy is a fundamental value in Microsoft's anti-botnet actions. When we execute an operation, we are required to work within the bounds of the court order. We never have access to email or other content of victim communications from infected computers. Instead, Microsoft receives the IP address used by the infected computers to identify the victims. We give domestic IP addresses to Internet service providers in the United States so they can alert their customers directly. We give the rest to the Computer Emergency Response Teams, commonly referred to as "CERTS," in countries where those victims are located. The owners are then notified of the infections and offered assistance in cleaning their computers.

In summary, through the course of anti-botnet operations, Microsoft has worked with partners to protect millions of people and their computers against malicious cyber criminals. This has led to the disruption and shutdown of some of the most menacing threats to public trust and security on the Internet. Cyber criminals continue to evolve their tactics. They keep developing more sophisticated tools to profit from the online chaos that they themselves create. We remain firmly committed to working with other companies and law enforcement to disrupt botnets and make the Internet a more trusted and secure environment for everyone.

Thank you for your time, Senator, and I am happy to answer any questions you may have.

[The prepared statement of Mr. Boscovich appears as a submission for the record.]

Chairman WHITEHOUSE. Ms. McGuire.

STATEMENT OF CHERI F. MCGUIRE, VICE PRESIDENT, GLOBAL GOVERNMENT AFFAIRS AND CYBERSECURITY POLICY, SYMANTEC CORPORATION, MOUNTAIN VIEW, CALIFORNIA

Ms. MCGUIRE. Chairman Whitehouse, thank you for the opportunity to testify today. I am especially pleased to be here with you again to focus attention on botnets and cybercrime and how industry and Government are working together to address these serious issues.

As the largest security software company in the world, Symantec protects much of the world's information, but botnets today are the foundation of the cyber criminal ecosystem. And as was discussed earlier, the uses for malicious botnets are only limited by the imagination of the criminal botmasters. These can range, as you mentioned, from distributed denial-of-service attacks to Bitcoin mining to distribution of malware and spam. Botmasters also rent out their botnets as well as use them for stealing passwords, credit card data, intellectual property, or other confidential information, which is then sold to other criminals.

Until now, virtually all botnets have been networks of infected laptop and desktop computers. However, in the past few years we have seen botnets made up of mobile devices, and we fully expect that the coming "Internet of Things" will bring with it a future of "thingbots," ranging from appliances to home routers to video recorders—and who knows what else.

Taking down a botnet is technically complex and requires a high level of expertise. But despite these obstacles, law enforcement and the private sector working together have made significant progress in the past several years.

Symantec's work to bring down the ZeroAccess botnet, one of the largest botnets in history at 1.9 million infected devices, is a good example of how coordination can yield results. ZeroAccess was designed for click fraud and Bitcoin mining, with an estimated economic impact of tens of millions of dollars lost per year. And the electricity alone to run that botnet cost as much as $560,000 per day.

One year ago today, Symantec began to sinkhole ZeroAccess infections, which quickly resulted in the detachment of more than half a million bots. This meant that these bots could no longer receive any commands and were effectively unavailable to the botmaster for updating or installing new revenue generation malware.

Another significant win came last month with the major operation against the financial fraud botnet Gameover Zeus, as several witnesses have testified to. As part of this effort, Symantec worked in a broader coalition to provide technical insights into the operation and impacts of this botnet. As a result, authorities were able to seize a large portion of the criminals' infrastructure.

In our view, the approach used in the Gameover Zeus operation was the most successful to date and should serve as a model for the future. A group of more than 30 international organizations from law enforcement, the security industry, academia, researchers, and ISPs all cooperated to collectively disrupt this botnet. This successful model of public and private cooperation should be repeated in the future.

While ZeroAccess and Gameover Zeus were successes for law enforcement and industry, there are undoubtedly more criminal rings operating today. Unfortunately, there are just not enough resources. As you said, so many botnets, so little time. As criminals migrate online, law enforcement needs more skilled personnel dedicated to fighting cybercrime.

At Symantec, we take numerous steps to assist victims of botnets and cybercrime and to aid law enforcement around the world. In the interest of time, I will mention only victimvoice.org, a new online assistance program that we unveiled in April with the National White Collar Crime Center. This site helps cybercrime victims file complaints and understand the investigation process. And in particular, I would like to thank you again, Senator Whitehouse, for your support and participation in that launch. It has already helped many victims of cybercrime.

To combat botnets and cybercrime, cooperation is key. In the private sector, we need to know that we can work with Government and industry partners to disrupt botnets without undue legal barriers. To be clear, I am not talking about a blank check. But consistent with privacy protections and legal parameters, we need to be able to share cyber threat information and coordinate our efforts quickly.

Information-sharing legislation will go a long way to do this. But it also must address the considerable privacy concerns and must include a civilian agency lead and data minimization requirements for both the Government and industry.

Last, the laws governing cybercrime should be modernized. In the U.S., we need to amend laws such as the Electronic Communications Privacy Act, the CFAA, and others that were written before our modern Internet and e-commerce was envisioned.

In addition, Mutual Legal Assistance Treaties and their process that allows governments to cooperate take far too long to address the real-time nature of international cybercrime and should be streamlined.

As this Subcommittee knows so well, we still face significant challenges in our efforts to take down botnets and dismantle cybercrime networks. But while there remains much work to be done, we have made progress.

At Symantec, we are committed to improving online security across the globe, and we will continue to work collaboratively with our customers, industry, and governments on ways to do so.

Thank you again for the opportunity to testify today, and I will be happy to answer any questions you may have.

[The prepared statement of Ms. McGuire appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you, Ms. McGuire, and thank you for Symantec's leadership in this area.

I am going to briefly recess the hearing and then return. We have a vote on the Senate floor that started 15 minutes ago, and I have 15 minutes to get there and vote, so I have zero time. But with any luck, that means I can get over there, vote, vote on the next vote, and then come right back. And then we will be able to proceed in uninterrupted fashion. So please just relax in place. It probably is going to be 5 to 10 minutes, and we will resume. Thank you.

[Whereupon, at 3:28 p.m., the Subcommittee was recessed.]

[Whereupon, at 3:45 p.m., the Subcommittee reconvened.]

Chairman WHITEHOUSE. All right. The hearing will come back to order. I appreciate everybody's courtesy while I got those two votes done.

And now, Dr. Vixie, we welcome your testimony. We welcome you here. Please proceed.

STATEMENT OF PAUL VIXIE, PH.D., CHIEF EXECUTIVE OFFICER, FARSIGHT SECURITY, SAN MATEO, CALIFORNIA

Mr. VIXIE. Thank you, Mr. Chairman. Thank you for inviting me to testify on the subject of botnets. I am speaking today in my personal capacity based on a long history of building and securing Internet infrastructure, including domain name system infrastructure. I am also here at the behest of the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), a nonprofit Internet security association whose international membership is actively working to improve the Internet security condition worldwide.

Let me start by reviewing some successful botnet takedowns in recent years, since they may prove instructive. They are successes, after all.

In 2008 the Conficker worm was discovered, and by mid-2009 there were over 10 million infected computers participating in this botnet. That was the largest to that time. I had a hands-on-keyboard role in operating the data collection and measurement infrastructure for the takedown team, in which competing commercial security companies and Internet service providers—most of which were members of M3AAWG—cooperated with each other and with the academic research and law enforcement communities to mitigate this global threat.

Then in 2011, the U.S. Department of Justice led “Operation Ghost Click” in which a criminal gang headquartered in Estonia was arrested and charged with wire fraud, computer intrusion, and conspiracy. The DNS Changer botnet included at that time at least 600,000 infected computers, and the mitigation task was made complicated by the need to keep all of these victims online while shutting off the criminal infrastructure the victims depended on. My employer was the court-appointed receiver for the criminal’s Internet connectivity and resources, and I personally prepared, installed, and operated the replacement DNS servers necessary for that takedown.

In each of these examples we see an ad hoc public-private partnership in which trust was established and sensitive information, including strategic planning, was shared without any contractual framework. These takedowns were so-called handshake deals where personal credibility, not corporate or government heft, was the glue that held it together and made it work. And in each case the trust relationships we had formed as members of M3AAWG were key enablers for rapid and coherent reaction.

Each of these takedowns is also an example of modern multilateralism in which intent, competence, and merit were the guiding lights. The importance of multilateralism cannot be overemphasized. We have found that when a single company or a single agency or nation goes it alone in a takedown action, the result has usually been catastrophe, because the Internet is richly interdependent and many of the rules governing its operation are unwritten.

Now, the ad hoc nature of these public-private partnerships may seem like cause for concern, but I hope you will consider the following:

First, this is how the Internet was built and how the Internet works.

Second, this is how criminals work with other criminals. We would not get far by trying to solve these fast-evolving global problems with top-down control or through Government directives and rules.

Let me explain what makes botnets possible. As you yourself pointed out in your opening remarks, a botnet is literally a network of robots, where by “robot” we mean a computer that has been captured and made to run software neither provided by the computer’s maker nor authorized or installed by its owner. Every Internet-connected device has some very complex software including an operating system, installed applications, and so forth. The only hard and fast requirement for any of this software is interoperability, meaning it merely has to work.

Now, the cost of the Internet’s spectacular growth is that much of the software we run was not adequately tested. The challenge for the Internet is that today there is perhaps more assurance that a UL-listed toaster oven will not burn down our house than there is that some of our vastly more expensive and powerful Internet-connected devices are insulated from becoming a tool of online criminals. These are consumer devices in a competitive and fast-moving market, so time to market is often the difference between success and bankruptcy.

This is a very brief overview, and I would like to leave you with the following thoughts:

Number one, the Internet is the greatest invention in recorded history, in my opinion, in terms of its positive impact on human health, education, freedom, and on every national economy.

Number two, the Internet is also the greatest invention in recorded history in terms of its negative impact on human privacy and freedom, as evidenced by the massive and continuing intrusions that have been described here today.

Number three, our democratic commitment to the rule of law has very little traction on the Internet compared to how it works in the real world. The Internet is borderless, and yet it carries more of the world’s commerce every year.

Number four, takedown of criminal infrastructure, including botnets, must be approached not just as reactions after the fact but also as prevention by attacking underlying causes.

Number five, the U.S. Department of Justice is the envy of the world in its approach to takedown and its awareness of the technical and social subtleties involved, and I want to give a special nod to NCFTA, a public-private partnership with strong FBI ties, located in Pittsburgh.

Number six, and finally, no legislative or regulatory relief is sought in these remarks. The manner in which Government and industry have coordinated and cooperated on botnet takedown efforts has underscored the effectiveness of public-private partnerships as currently practiced in this field.

Mr. Chairman, this concludes my oral statement. Thank you for this opportunity to speak before you, and I would be happy to answer your questions.

[The prepared statement of Mr. Vixie appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you very much.

Finally, Mr. Spiezle. But before I let you begin your statement, my apologies for the mispronunciation earlier. And let me also say that, without objection, everybody’s complete statements will be made a part of the record, and I appreciate the abbreviated version that allows the testimony to proceed expeditiously at the hearing.

STATEMENT OF CRAIG D. SPIEZLE, EXECUTIVE DIRECTOR AND FOUNDER, ONLINE TRUST ALLIANCE, BELLEVUE, WASHINGTON

Mr. SPIEZLE. Thank you very much. Chairman Whitehouse, Ranking Member Graham, and Members of the Committee, thank you for the opportunity to testify before you today. I also would like to thank you for your leadership in focusing attention to this important topic which is impacting users and businesses throughout this country.

My name is Craig Spiezle, and I am the executive director and president of the Online Trust Alliance. OTA is a global nonprofit, with the mission to enhance online trust and empower users, while promoting innovation and the vitality of the Internet.

Botnets pose a significant risk to businesses and governments, and one of my specific concerns is the impact to small and medium businesses that are often defenseless. Increasingly bots are deploying loggers, malvertising, and ransomware driving identity theft and bank account take-overs and holding users and their data hostage.

It is important to recognize that fighting bots is not a domestic issue. Criminals are leveraging the jurisdictional limitations of law enforcement and often operate with impunity. Left unabated, they are a significant threat to our Nation's critical infrastructure and to our economy.

In my brief testimony, I will touch on five key areas: status of industry efforts, a holistic anti-bot strategy, the role and issues of takedowns, the role of data sharing, and the importance of privacy safeguards.

I should note efforts to combat botnets have been embraced by a range of public and private efforts. An example is the FCC's Communications Security, Reliability and Interoperability Council (CSRIC), which last year developed a voluntary Anti-Botnet Code of Conduct for ISPs. This is a first step and example of the industry's ability to self-regulate.

In parallel, the OTA has facilitated several multi-stakeholder efforts, bringing in leaders throughout the world. We have published specific remediation and notification best practices and anti-bot guidelines for hosters and cloud service providers. The initial adoption of these practices are now paying dividends helping to protect users' data and their privacy.

Fighting botnets requires a global strategy. As outlined here in Exhibit A, OTA advocates a six-pronged (1) framework, (2) prevention, (3) detection, (4) notification, (5) remediation, and (6) recovery. Within each one of these, we have outlined a partial list of tactics, which underscores the increased need for collaboration, research, and data sharing between both the public and private sectors.

In the bottom of this slide, it points out the role of consumers and education. We need to help them update their device and look to how we can help educate them on the risks of botnets.

As outlined, law enforcement is an important part here as well, and it serves three major functions: disrupting cyber criminals, gathering intelligence, and bringing criminals to justice.

But law enforcement cannot act on this alone. A trusted partnership is required, and progress has been made with industry leaders, including Microsoft, Symantec, and others.

But takedowns need to be taken with respect to three major considerations: one, the risk of collateral damage; two, the errors in identifying targets for mitigation; and, three, the importance of respecting users' privacy. For example, when taking down a web hoster because they have a handful of bad customers, there is a risk of collateral damage. At the same time, service providers cannot hide behind bad actors, and they must take steps to prevent the harboring of such criminals.

It is also important to note that all anti-abuse and security tactics all run similar risks. The anti-spam community often blocks legitimate senders. Web browsers can misidentify phishing sites and AV solutions can mistakenly block downloads. Recognizing these possibilities, risk assessment procedures must be pre-established with processes in place to remediate any unintended impact.

Data sharing has the promise of being one of the most impactful tools in our arsenal, yet it must be reciprocal. Collaboration is required in all sectors, including retail, financial services, and advertising. In this void, criminals move from one industry to another, sending malicious spam one day and perpetrating click fraud and malvertising the next.

The privacy landscape is also rapidly evolving, creating perceived obstacles to data sharing. Privacy needs to be at the foundation of all fraud prevention and data-sharing practices. I believe these can be easily addressed. When data is used and collected for threat detection, entities should be afforded a "safe harbor." Conversely, industry needs assurances that law enforcement will not use any data for any other purposes.

As Exhibit A outlines, every stakeholder has a responsibility. Progress has been made, but a renewed commitment needs to be required by all stakeholders. As the Internet of Things, mobile, the smart grid, and wearable technologies becomes prevalent, we need to look beyond the desktop.

In summary, it is important to recognize that there is no absolute defense. Both the public and private sectors need to increase investments in data sharing and adopt privacy-enhancing practices while finding new approaches to work with law enforcement and expand international cooperation. Working together we can make the Internet more trustworthy, secure, and resilient.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Spiezle appears as a submission for the record.]

Chairman WHITEHOUSE. Thank you very much, Mr. Spiezle, and thank you all.

Let me start with a question that I will ask each of you for the record, which means if you could provide a written response, and that is that, as you have heard, Senator Graham and I are working on legislation in this area. As you heard from the first panel, the Department of Justice and the Federal Bureau of Investigation have a number of suggestions. I would like to ask you to provide your comments, if any, to the suggestions that have been made so far and add any suggestions that you may have of your own for this legislation so that we can build a good legislative record to support our proposal going forward.

[The information referred to appears as a submission for the record.]

Chairman WHITEHOUSE. I am also interested in your thoughts. As a lay person, it strikes me that botnets are becoming more dangerous, that their capabilities are growing. My first exposure to botnets was when they were spam propagators, and then they became distributed denial-of-service vectors to swamp individual websites. But now they seem—so many additional capabilities have been listed in this hearing, right up to and including having people spy on you through your webcam on your computer while you are going about your business and tracking your keystrokes individually so that they can know your passwords and have access to your accounts.

Is my lay reading that botnets are becoming more dangerous or the criminals behind them are learning more dangerous capabilities a correct one? And what do you think the rate is of that change, if I am correct? Let me start with Mr. Boscovich.

Mr. BOSCOVICH. Yes, Senator, I think the observation is correct. I think that we are seeing an ever-changing sophistication on the part of cyber criminals.

I would like to point out one particular case which really demonstrates how creative cyber criminals are, and in this particular case, which was the Bamital case, if my memory serves me correctly, one of our industry partners was Symantec on that case. It was a case in with the botherders had actually developed code which actually took a step backward. And one of the reasons why they did that is because technical countermeasures that had been put in place by Bing, Google, and other companies to detect click fraud relied upon a certain type of algorithm. The criminals understood that, and they had to reintroduce a human element into their code. In essence, what they did is that they have changed their code, and they took one step back to take two steps forward in such a way that now the user would actually be using his mouse or her mouse, and while he or she thought he was actually clicking or looking for something, the reality was that they were, in fact, clicking on ads that the user was not even seeing, was appearing behind the screen that they were looking at, introducing a certain variation that was consistent with human behavior.

So the observation that criminals are, in fact, always learning, always changing, is an accurate one, and I think this example really underscores how sophisticated these cyber criminals are.

Chairman WHITEHOUSE. And in both dimensions. I mean, in terms of if you view a botnet as an infrastructure for criminal activity, it is one that has to be maintained and groomed, and they are getting more sophisticated at that. They are also getting more sophisticated at the type of criminal payload, if you will, that they deliver through that botnet as well. Is that correct, Ms. McGuire?

Ms. MCGUIRE. That is correct. I think your summary is quite accurate, that these have begun to progress and become much more sophisticated over the last 5 years. For example, the type of technology or infrastructure that they are using now, moving from central command and control, simple command and control servers to peer-to-peer networks, which are much more difficult to take down because of their complexity, is the type of morphing that we are seeing by the cyber criminals to use all avenues at their availability.

Chairman WHITEHOUSE. Dr. Vixie, you mentioned that in the face of this threat, prevention was something that we should be looking at, and you used the phrase in your testimony "underlying causes," that we should be prepared to address the underlying causes that allow this to occur even before the harm of a particular botnet is made manifest.

What did you mean by "underlying causes"? And what would you recommend, if anything, that we do to get ahead of this more by going after those underlying causes, as you have defined them?

Mr. VIXIE. I think that the reason that botnets have gotten stronger is because our computers have gotten stronger, better CPUs, more memory, more storage, et cetera. Our network has also gotten stronger, so it is possible to get a lot more work done with each computer you steal now compared to 5 years ago or 5 years before that.

If we wanted to start kicking the dependencies under botnets, we would need to somehow address the lack of testing. I mentioned in my written remarks that this last week there was an Internet of Things, I think it was a wireless light bulb that has a terrible security flaw in it, and I understand how that can happen. I have tried to get things—software products out the door myself, and it is difficult to say let us hold it back for another couple of weeks while we try to attack it every which way. Really what you want to do is get it out there and put it in customers' hands and so forth.

That is not going to work. We have got to find a way to test this software the way the bad guys do. We have to do the so-called Red Team test where you try to break in, and if you can, you get some sort of internal prize. We have got to find a way to encourage that.

Chairman WHITEHOUSE. So when electricity was the new technology and people were trying to get stuff out the door that caught fire if you left it on too long, as you pointed out, with respect to the toaster, Underwriters Laboratories was established to make sure that appliances met basic standards, and as a result, toaster fires and things like that have not been a very prominent concern for Americans for quite some time.

Do you think that an equivalent to an Underwriters Laboratories is possible on the Internet? And how would you see it as being overseen?

Mr. VIXIE. I do not think a direct equivalent is possible. When you are doing this kind of testing, you are looking for combinations and permutations of sort of how you set the knobs, what you put in the toaster, other conditions. And, you know, every one of those conditions is a State variable, and the problem is that my laptop has more complexity of that kind than all the computers on the planet had 30 years ago. And so coming up with a direct analog of the way UL tests our electric devices I think is misleading. I think standards in software development, standards in testing, possibly getting away from some of the older programming languages that almost encourage the type of defects that we see in our monthly updates are going to be better approaches. But I do want to say——

Chairman WHITEHOUSE. How would those approaches be administered?

Mr. VIXIE. Excuse me?

Chairman WHITEHOUSE. How would those proposals be best administered? Through the Government? Through the Internet governance system? Through a rating that you can advertise you have on your product if you have been through it voluntarily?

Mr. VIXIE. In that sense, the Underwriters Laboratories system is perfect because it is voluntary. If you want to sell a device that is not listed, then that is up to you. And if people would not buy as many—if fewer people want to buy it because it does not have that stamp, that is up to them. So I think there is room for someone to step into that role, but it is not a Government role.

Chairman WHITEHOUSE. Got you. And, Mr. Spiezle, you said that you felt that there were steps that consumers, individuals, could take to better acquaint themselves with this threat and to better protect themselves from this threat. What would your recommendations be? This seems like such a giant and complex and very high tech type of crime, and if you are an innocent user of your own computer going about your own business and doing what you are good at, which may not be anything to do with computers, how can you—what sensible steps should people be thinking about who are not computer whizzes to defend themselves and their computers?

Mr. SPIEZLE. Let me clarify. My point is that we all have a shared responsibility, not unlike driving a car. We have a responsibility of driving safely. We need to make sure our car is maintained and we have new tires on it. That was the point there.

I think realistically, though, education has a limited effect here. These attacks are—social engineering exploits are very hard to identify. They are drive-by, so just by their very nature of going to a trusted website that someone types in a URL, there can be malicious ads served on them. So it is a shared responsibility, but I do not put the faith that education is going to be the solution, but it should be one part.

I do want to address one point in your original question about the sophistication. Clearly, in the technical aspect, botmasters are more and more sophisticated. They are leveraging big data, data mining capability and analytics. So that adds to the profitability. Their ability to use that data, append data from other sources, and then trade in the underground economy makes it very profitable. They have become very nimble, become good marketers in a sense, and they are learning from business. So those are some of the challenges we must address.

Chairman WHITEHOUSE. Two final questions. The first is that many of the perpetrators in this area are foreigners, and we are obviously going to work with the Department of Justice and the Federal Bureau of Investigation to make sure that they have the capabilities that they need to be as strong as they can be in terms of pursuing foreign criminals. But none of you are involved as law enforcement officials. You are involved representing private companies and organizations, and in that sense, when you bring a civil action to close down a botnet, you may have civil remedies against individuals overseas that are different than what a prosecutor would be looking at.

Are there recommendations that you would have as to how we could strengthen overseas enforcement against the individuals and organizations that are running the botnets that would supplement just the technical capability to take down the botnets? Let me start with you, Mr. Boscovich.

Mr. BOSCOVICH. Well, Senator, I think that obviously as a private company, as you mentioned, our main sphere of influence is only using the civil process, and even in the civil process, once we get default judgments, there actually is a procedure in which we could seek to, for example, localize a U.S. judgment overseas. But it is a complex and lengthy process.

In all of the actions that we take with our partners, we then go ahead and always refer the cases and the evidence that is the basis of the information that we arrive at through the civil process to law enforcement. The process that law enforcement uses, of course, has been around for quite some time, and I believe some of the representatives of DOJ and the FBI were here earlier today, and they made references to the MLAT process and things of that sort. And these are procedures that have been around for a very long time. And in terms of how quickly these things could turn around, there has always been a question. I could only talk about my experiences when I was at Justice, that it does take time to turn this information request around.

But from the civil perspective, I think——

Chairman WHITEHOUSE. Particularly if the coordinating country is of two minds as to how much they want to take down this industry.

Mr. BOSCOVICH. Well, that is why the partnership, the private and public partnership is important, because what we try to focus on, of course, is the immediate cessation of the harm to people on the Internet. And to sever that communication, to stop the harm, and then notify the victims and then try to do something to remediate and clean their computers, working through ISPs and country CERTs, that is the job that we believe we can do, and do very well, with industry partners and with the Government as well.

In terms of the criminal side, I would have to defer to, you know, my former colleagues at the Justice Department.

Chairman WHITEHOUSE. No, I was thinking more of the civil side and pursuing personal liability and accountability of foreigners who have done harm to your companies.

Ms. McGuire, any thoughts on that?

Ms. MCGUIRE. Just this week we have seen reports, for example, that Gameover Zeus, that modifications to that particular malware are already being used by a new criminal gang or perhaps the original perpetrator, who fled to Eastern Europe, to launch new criminal activity. This is the kind of thing where, if we had a faster, speedier MLAT process, we could potentially address these kinds of issues at the speed of the Internet as opposed to what I have been told by law enforcement partners can take anywhere from 6 months to never.

And so those are the kinds of enhancements, modernizations to these international treaties that we really need in order to go after——

Chairman WHITEHOUSE. Again, you are comfortable relying on the law enforcement process for that and at this point do not have any interest in pursuing civil liability on the part of your private sector companies against foreign individuals to—as a deterrent or to recover for the damages that they have caused you?

Ms. MCGUIRE. Most of our activity is on the sharing of information and notification to both our international law enforcement and CERT partners so that they can then take the action that they need within their jurisdictions.

Chairman WHITEHOUSE. And what have each of you seen in terms of the coordination that has been your experience between the private sector and between law enforcement? It has emerged, and it seems to me from what I hear to be in a pretty good place right now. There are a number of mechanisms through which the FBI in particular but other Federal law enforcement agencies cooperate with the private sector and exchange information and deconflict activities. I think there has been a lot of improvement there, but I would like to hear from each of you how close you think we are to what we should be doing and whether there is any specific recommendations you have. Let me start from this side, Mr. Spiezle.

Mr. SPIEZLE. Thank you. I think we have had great success, but I think there is a whole other layer of information sharing that we are not getting today, and we need to bring other data sources together. So more data sharing between the financial services, and certainly we are seeing progress with the FS-ISAC. We are seeing more breaches experienced in the retail sector. We get data from them. And the reason this is important is it is connecting the dots. And so it is not always just from the ISPs and other sectors. So we need to get that. We need to open the dialogue, but also to remove the burden of whether it is antitrust, the concerns of privacy, or the concerns of regulatory authorities coming after them. So how do we open up that dialogue even domestically so we can get a higher level of granularity and telemetry from other data sources?

Chairman WHITEHOUSE. Dr. Vixie.

Mr. VIXIE. So I mentioned in my remarks that the Internet is borderless, and you mentioned in this question that the criminals are borderless, and I think that firmly points to the fact that our solutions have to be borderless. So I will say again NCFTA in Pittsburgh has a huge international outreach program. I go and do some training there of the international law enforcement community every summer. But they do it year-round, and it is a huge thing, because a lot of the other countries where the cybercrime is originating right now do not have the capability to train their people locally. They do not necessarily have the budget for the tools that are needed and so forth. So I think I really want to encourage more outreach of that kind, possibly not just by NCFTA but by other U.S. agencies who are leading in the world.

I do not have an answer for civil lawsuits. I know that it can be used if you are trying to get at somebody and you do not know who they are. You can often get a court order using a John Doe. But it is messy, and it has not really produced consistent results.

Chairman WHITEHOUSE. Ms. McGuire.

Ms. MCGUIRE. I would also echo that the NCFTA is a terrific organization, particularly on the international front, as well as working with industry and between law enforcement partners and Government agencies. But in particular to your question on information sharing and has it gotten better with the FBI and the Department of Justice, we have seen significant improvements, frankly, over the last 2 years in our ability to work with them, their responsiveness to the information that we are sharing with them about indicators of compromise, about just the process that they are using. And as I think I mentioned earlier, Gameover Zeus we think is the best example so far where they reached out to more than 30 international organizations, including industry, governments, researchers, ISPs, brought all of them together so that collectively we could be ready and work the takedown once the injunctions and the appropriate actions were taken.

So that is, I think, the model——

Chairman WHITEHOUSE. The borderless response, to Dr. Vixie's point.

Ms. MCGUIRE. Yes, borderless response, exactly. And I think that is the model we need to work toward in the future, and we have one now as a proof point for the future.

Chairman WHITEHOUSE. Mr. Boscovich, last thoughts.

Mr. BOSCOVICH. I think deconfliction is one of the key components of a successful private-public partnership, and in cases such as Citadel, Gameover Zeus, and more recently the Shylock-Capshaw operation recently that went down in Europe is a perfect example of public-private partnerships, civil process complementing criminal process, all while stopping the harm immediately, working to help the victims, yet at the same time allowing the criminal side to do what they do best, the deterrent effect, going out and arresting individuals. And I think that we have come a long way in getting at that sweet spot where we now have an appropriate mechanism by which we share information, where we deconflict with law enforcement, both domestically and internationally, to achieve the greatest impact possible in these takedowns.

Chairman WHITEHOUSE. Thank you very much.

A final good word to Microsoft, just lawyer to lawyer. You were among the earliest companies—probably all three of you were involved over the years; a lot of people were connected to Microsoft here—in the first civil takedowns, and just as a lawyer, to read those early complaints and see the statutory grounds based on very modern, complicated electronic privacy statutes, and at the same time doctrines of English common law that were transplanted to America when we formed our country and that are part of the common law history dating back to the 1400s side by side as a separate count, it was—it must have been a lot of fun. It was terrific legal work, and it had a wonderful effect. So I compliment you on it. And I assume that you would want—you know, we are legislators, and so we think about legislating. It is like the story about the hammer. Every solution that a hammer sees requires a nail. And so we tend to think in terms of new and amended statutes. But I gather you would want to make sure that we left room for traditional common law remedies to maintain themselves as a part of the repertoire here and to allow the natural development that the common law permits. Is that fair to say?

Mr. BOSCOVICH. Absolutely, Senator. One of the beauties behind the common law system is its ability to adapt constantly to new facts. And what we are looking at here is a threat which is constantly adapting, something that is always moving, always morphing. And the beauty behind common law and trespass to chattels, tortious interference with a contractual relationship, these are theories that we could use over and over again and are part of a system that in it at its core is able to adapt quickly. So, yes, I think that I would love to see the standard common law principles remain intact as we tackle these.

Now, having said that, it does not mean that there is not always room for improvement in both present statutes and potentially even new statutes. And we would gladly take a look at any type of amendment and/or proposed legislation that Congress and yourself may have and give our comments so that you could have the best insight possible, from us at least.

Chairman WHITEHOUSE. Well, certainly when they first came up with trespass upon chattels, it was well before anybody had an inkling there could ever be an Internet, so that certainly has been a lasting doctrine.

Let me thank all of the witnesses for this hearing. I appreciate very much your input. I look forward to the responses to the question for the record. I think that we have a very strong, bipartisan group of Senators who are very interested in this issue and are looking forward to coming up with legislation that can pass and help you all in your important pursuits to protect our economy and your clients and your companies from the kind of attacks that we are seeing, largely from overseas.

So Godspeed to you all in your work. Thank you very much for what you have done and for your testimony today. We will keep the record open for 1 week for anybody who cares to add anything to the record and for those question-for-the-record responses to come in.

And, with that, we are adjourned.

[Whereupon, at 4:24 p.m., the Subcommittee was adjourned.]

[Additional material submitted for the record follows.]

APPENDIX

Additional Material Submitted for the Record

Witness List

Hearing before the
Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism

On

"Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks"

Tuesday, July 15, 2014
Dirksen Senate Office Building, Room 226
2:30 p.m.

Panel I

The Honorable Leslie Caldwell
Assistant Attorney General, Criminal Division
United States Department of Justice
Washington, DC

Joseph Demarest, Jr.
Assistant Director, Cyber Division
Federal Bureau of Investigation
Washington, DC

Panel II

Richard Boscovich
Assistant General Counsel, Digital Crimes Unit
Microsoft
Redmond, WA

Cheri McGuire
Vice President, Global Government Affairs & Cybersecurity Policy
Symantec Corporation
Mountain View, CA

Dr. Paul Vixie
Chief Executive Officer
Farsight Security
San Mateo, CA

Craig Spiezle
Executive Director
Online Trust Alliance
Bellevue, WA

Department of Justice

STATEMENT OF

LESLIE R. CALDWELL
ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIME AND TERRORISM
UNITED STATES SENATE

AT A HEARING ENTITLED

"TAKING DOWN BOTNETS: PUBLIC AND PRIVATE EFFORTS TO DISRUPT AND DISMANTLE CYBERCRIMINAL NETWORKS"

PRESENTED
JULY 15, 2014

Statement of
Leslie R. Caldwell
Assistant Attorney General
Criminal Division
Department of Justice

Before the
Committee on the Judiciary
Subcommittee on Crime and Terrorism
United States Senate

At a Hearing Entitled
"Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks"

Presented
July 15, 2014

Good afternoon, Chairman Whitehouse, Ranking Member Graham, and Members of the Subcommittee. Thank you for the opportunity to appear before the Subcommittee today to discuss the Department of Justice's fight against botnets. I also particularly want to thank the Chair for holding this hearing and for his continued leadership on this important issue.

The threat from botnets—networks of victim computers surreptitiously infected with malicious software, or "malware," that are controlled by an individual criminal or an organized criminal group—has increased dramatically over the past several years. The computers of American citizens and businesses are, as we speak, under attack by individual hackers and organized criminal groups using state-of-the-art techniques seemingly drawn straight from a science fiction movie. Unfortunately, this cybercrime wave is all too real. Botnet attacks are intended to undermine Americans' privacy and steal from unsuspecting victims. If left unchecked, they will succeed.

The Department of Justice, working through highly trained prosecutors and Federal Bureau of Investigation (FBI) agents, recognizes this threat, and is working day and night to protect our citizens, our national security interests, and our businesses. We responsibly employ the investigative and remedial tools Congress has given us, and we leverage our strengths by teaming up with partners across the federal government and, where appropriate, in the private sector and foreign law enforcement. As in the recent disruption of the Gameover Zeus botnet, which I will discuss more later, we find ourselves matched against increasingly sophisticated cyber criminals, and must evolve our tools and tactics minute-by-minute to prevent further harm to innocent victims.

Our successful effort to suppress the Gameover Zeus botnet should remind us that those who use botnets to cause harm are increasing in number and sophistication, and we cannot expect continued success if we merely rest on our laurels. The Department is armed with the laws and resources that we have been granted, but those tools must be updated and enhanced. If we want to remain effective in protecting our citizens and businesses, our laws and our resources must keep pace with the tactics and numbers of our adversaries. Our adversaries are always adapting. So must we. In my testimony, I will outline several legislative proposals that will assist the Department in its efforts to counter the threat posed by botnets. Finally, I will outline our resource needs—in particular the need for additional specialized criminal prosecutors.

Current DOJ Anti-Botnet Activities

Cybercrime overall has increased dramatically over the last decade, and caused enormous financial damage and innumerable invasions of Americans' privacy. The advances in computing technology that have powered our economy have also empowered those who seek to do us harm. Today, cyber criminals can steal personal and financial information from tens of millions of citizens in a single breach. To be sure, thefts of such information were committed long before the digital revolution. But stealing ten million credit card numbers previously would have required burglarizing thousands of stores, whereas now it can be done from a basement with a laptop. And some crimes have been uniquely adapted in the digital age. For example, in a new, disturbing twist on extortion, hackers have secretly activated the cameras on victims' laptop computers, taken compromising pictures or videos, and demanded payments not to expose those pictures or videos to the public. All the while, technological advances, including advances designed to protect privacy, such as anonymizing software and encryption, are being used to frustrate criminal or civil investigations and, perversely, protect the wrongdoers. Our cyber crimefighters must be equipped with the tools and expertise to compete with and overcome our adversaries.

Over the same time period, botnets have emerged as a major threat. Sometimes called "botmasters" or "botherders," cyber criminals who control botnets can use advances in communications technology to take control of thousands, or even hundreds of thousands, of victim computers, or "bots." They can then command the computers they control to, for example, deluge an internet site with junk data, overwhelming it and knocking it offline. They may conduct such distributed denial-of-service (DDOS) attacks out of malice, as ideological attacks on those with whom they disagree, or even as a paid service to other criminals. They can also use the infected bots to steal banking credentials, credit card numbers, and other financial information. They can use them to send spam—email messages that range from advertising for illegal and dangerous pharmaceutical products, to fraud schemes aimed at artificially inflating the price of stocks, to "phishing" messages that gather sensitive information. Moreover, cybercriminals can use botnets to engage in other online crime by using their networks of infected computers as "proxies." This activity allows such criminals to conceal their identity and location while they commit crimes that range from fraud and theft of data to drug dealing and the sexual exploitation of children.

Botnets pose a threat to the United States, our citizens, and our businesses that must not be underestimated. By hijacking numerous victims' identities, credit cards, and bank accounts, criminal groups already have stolen hundreds of millions of dollars. And every day cyber criminals violate the privacy of Americans on a staggering scale, by stealing financial information, personally identifiable information, login credentials, and other information from victims who often do not even realize their computers have been compromised. Because botnets can be so lucrative, their designers use sophisticated code, locate their servers in countries around the world, and employ the latest in encryption methods—all designed to frustrate personal and corporate cybersecurity efforts, and to prevent law enforcement from responding effectively. Indeed, recent cases and ongoing investigations reveal that botnets are used by criminals halfway around the world to commit crimes of a scope and sophistication that was difficult to imagine only a few years ago.

To counter this significant and complex threat, the Justice Department is vigorously responding to botnets and other cybercrimes through the tenacious work of the Criminal Division's Computer Crime and Intellectual Property Section, also known as CCIPS, and the Computer Hacking and Intellectual Property Coordinators and National Security Cyber Specialists in U.S. Attorneys' Offices across the country. These prosecutors, along with colleagues in the National Security Division (NSD), form a network of almost 300 Justice Department cybercrime prosecutors. In addition, the FBI has made combating cyber threats one of its top national priorities, working through Cyber Task Forces in each of its 56 field offices and continuing to strengthen the National Cyber Investigative Joint Task Force. The FBI has also moved aggressively to counter the botnet threat through Operation Clean Slate, a major FBI initiative designed to identify and eliminate the most significant criminal botnets. The United States Secret Service also focuses on cyber threats to financial networks and the personal financial information of Americans. Through a network of 35 Electronic Crimes Task Forces across the country and in key foreign countries, Secret Service investigations have resulted in the arrest and successful prosecution of the criminals responsible for some of the largest data breaches. U.S. Immigration and Customs Enforcement, Homeland Security Investigations (HSI), through the HSI Cyber Crimes Center (C3), has also dedicated significant resources to equip its Special Agents with the tools and knowledge necessary to combat transnational cybercrime.

The Department's response to botnets takes two tracks, often at the same time. First, whenever possible, we seek to arrest, prosecute, and incarcerate the criminals who use botnets to victimize Americans. For example, in January 2014, Aleksandr Andreevich Panin, a Russian national, pled guilty in federal court in Atlanta, Georgia to conspiracy to commit wire and bank fraud for his role as the primary developer and distributor of the malicious software known as "SpyEye." According to industry estimates, SpyEye has infected over 1.4 million computers in the United States and abroad. SpyEye secretly infected victims' computers and enabled cyber criminals to remotely control them through command and control servers. Designed to automate the theft of confidential personal and financial information, such as online banking credentials, credit card information, usernames, passwords, PINs, and other personally identifying information, SpyEye was the preeminent malware toolkit used from approximately 2009 to 2011. Panin sold versions of the SpyEye virus to other criminals for prices ranging from $1,000 to $8,500. Panin is believed to have sold the SpyEye virus to at least 150 "clients" who, in turn, used it to set up their own botnets. One of Panin's clients alone was reported to have stolen over $3.2 million in a six-month period using SpyEye. Panin is awaiting sentencing, and four of his clients and associates were arrested by foreign law enforcement agencies.

Similarly, in federal court in New York in May 2014, Michael Hogue pled guilty, and an indictment was unsealed against Alex Yucel, in connection with their development of a particularly insidious piece of computer malware known as Blackshades. This malware was sold and distributed to thousands of people in more than 100 countries and was used to infect more than half a million computers worldwide. Once installed on a computer, the malware could collect the user's financial information and even turn on the computer's camera to spy on the unsuspecting user. An individual who helped market and sell the malware and two Blackshades users who bought the malware and then unleashed it upon unsuspecting computer users were also charged and arrested in the U.S. The charges and guilty plea were part of a law enforcement operation involving 18 other countries. More than 90 arrests have been made so far, and more than 300 searches have been conducted worldwide.

Arresting and convicting key players can disrupt criminal enterprises, but such actions are not always sufficient to counter the threat, particularly given the transnational nature of cybercrime. They also will not always remedy the harm caused by a botnet. Accordingly, the Department has pursued a second approach to botnets: the use of seizures, forfeitures, restraining orders, and other civil and criminal legal process to dismantle criminal infrastructure. In cases such as Gameover Zeus, Blackshades, and a 2011 case involving the Coreflood botnet, the Department used these legal authorities, with judicial authorization and oversight, to wrest domains and servers from cyber criminals' control, prevent infected computers from communicating with the criminals' command and control infrastructure, and liberate hundreds of thousands of computers.

In May of this year, CCIPS, the United States Attorney for the Western District of Pennsylvania, and the FBI, in partnership with other federal and private-sector organizations, disrupted a botnet that illustrates the magnitude of the threat. Before it was disrupted, the Gameover Zeus botnet was widely regarded as the most sophisticated criminal botnet in existence. One common and sinister method used by Gameover Zeus was a "man-in-the-middle" attack, in which victims trying to access websites for purposes such as online banking were tricked into entering login credentials, passwords, and other personal information that communicated that information to criminals at the same time they were passed onto their destination. With the click of a mouse, the botmasters then used this stolen information to rob small businesses, hospitals, and other victims, transferring funds from victim accounts to their own accounts. From September 2011 through May 2014, Gameover Zeus infected between 500,000 and 1 million computers and caused more than $100 million in financial losses. In one case alone, nearly $7 million was fraudulently transferred from a regional bank. Other victims included an Indian tribe, a corporation operating assisted living facilities, and a composite materials company.

Gameover Zeus was also used to install Cryptolocker—a type of malware known as "ransomware"—on infected computers. Cryptolocker enabled cyber criminals to encrypt key files on the infected computers. Victims then saw a splash screen on their computer monitors, telling them that their files were encrypted and that they had three days to pay a ransom, usually between about $300 and $750, if they wanted to receive the decryption key. The victims found themselves confronted with the loss of critical data, such as family photographs or essential business records. In the short period between its emergence in mid-to-late 2013 and the disruption action in May 2014, the Cryptolocker malware infected more than 260,000 computers worldwide. Many victims simply paid the ransom that was demanded of them. These victims included the police department of Swansea, Massachusetts, which paid approximately $750 to recover its investigative files and arrest photographs. Others refused to pay the ransom and tried to defeat the malware. A Pittsburgh insurance company was eventually able to restore data from a backup, but only after incurring an estimated $70,000 in losses and sending employees home during remediation. A Florida company lost critical files, which resulted in an estimated $30,000 in loss. And a North Carolina business, whose main files and backup were both encrypted, lost its critical files despite engaging a computer forensics firm to try to restore its access. That company has lost about $80,000, and the owner told the FBI that he may have to lay off employees as a result.

Disrupting and mitigating these threats requires determination, technical skill, and creativity. In response to previous efforts to disable botnets, the creators of the Gameover Zeus botnet designed a novel and resilient structure, including three distinct layers of command and control infrastructure that rendered the botnet particularly difficult to overcome. The Department's successful disruption began with a complex international investigation conducted in close partnership with the private sector. It continued through the Department's use of an inventive combination of criminal and civil legal process to obtain authorization to stop infected computers from communicating with each other and with other servers around the world. The operation simultaneously targeted all three command and control layers of Gameover Zeus, and stopped Cryptolocker from encrypting additional computers. The investigation and court-authorized operation ultimately permitted the team not only to identify and charge one of the leading perpetrators, but also to stop the botnet and ransomware from functioning. Moreover, the FBI was able to identify victims and, working with the Department of Homeland Security, foreign governments, and private-sector partners, facilitate the removal of malware from many victim computers. Disclosure to, and engagement with, the public was critical to this remediation effort. DOJ and DHS released a technical alert to raise awareness of the botnet and lay out resources available to help affected entities minimize the damage.

I cannot emphasize enough the importance to our anti-botnet efforts of the cooperation of foreign governments and our U.S. government and private-sector partners. In every case I have mentioned, foreign law enforcement services took carefully coordinated steps worldwide to disrupt the scheme and investigate the offenders, by seizing servers, interviewing subjects, making arrests, and providing evidence to U.S. investigators. The Department has devoted substantial resources to building the relationships with foreign law enforcement partners that made these coordinated efforts possible. The FBI, for example, maintains more than 60 legal attachés in embassies around the world. The Criminal Division's Office of International Affairs provides immeasurable legal support to evidence collection and extradition. CCIPS conducts training programs to help our allies develop cyber laws, and our federal law enforcement partners work to improve investigative capacities. Due in large part to our extensive engagement with, and training of, foreign criminal prosecutors and law enforcement officers, we have developed highly productive international relationships that are critical to the success of our investigations and prosecutions.

One factor has harmed our relationships with foreign law enforcement agencies, however: our inability to rapidly respond to foreign requests for electronic evidence located in the United States. Our capacity to do so simply has not kept up with the demand. The President's budget for fiscal year 2015 requests additional prosecutors, together with support personnel, to be assigned to the Criminal Division and to United States Attorneys' Offices to streamline and facilitate the process of handling Mutual Legal Assistance Treaty (MLAT) requests between the United States and its law enforcement partners around the world. The FY 2015 request, if granted, will enable the Department to meet the Administration's commitment to cut MLAT response times in half by the end of 2015 and reduce the amount of time to comply with legally sufficient requests to a matter of weeks, as well as to strengthen the Department's relationships with our foreign law enforcement partners, particularly in regard to cyber investigations.

Like the value of our relationships with foreign law enforcement, the expertise, dedication, and cooperation of private-sector entities have been crucial to our success. For example, security researchers develop highly specialized expertise in particular botnets and help develop countermeasures that match the botnets in sophistication. Their technical contributions are truly astounding. Private-sector companies also serve a critical function when they notify victims that their computers have been compromised and supply the tools needed to clean up those computers. Because the vast majority of the internet is owned and operated by the private sector, we simply could not conduct anti-botnet operations without the firm commitment of network service providers to protecting their customers.

Proposals to Enhance Anti-Botnet and other Cyber Capabilities

The Department is dedicated to using innovative means to target increasingly complex botnet threats as they emerge. But there is a lot more work to be done, and we ask that Congress continue its support of these critical efforts. I would like to highlight some of the Department's legislative and budgetary proposals that would enhance our ability to identify botnet perpetrators, bring them to justice, disrupt their criminal enterprises, and protect the security, privacy, and property of Americans.

Department prosecutors rely on criminal statutes to bring cyber criminals to justice and to halt their criminal activity. One of the most important of these laws is the Computer Fraud and Abuse Act, also called the "CFAA." The CFAA is the primary Federal law against hacking. It protects the public against criminals who hack into computers to steal information, install malware, and delete files. The CFAA, in short, reflects our shared baseline expectation that people are entitled to have control over their own computers and are entitled to trust that the information they store in their computers remains safe.

The CFAA was first enacted in 1986, at a time when the problem of cybercrime was still in its infancy. Over the years, a series of measured, modest changes have been made to the CFAA to reflect new technologies and means of committing crimes and to equip law enforcement with tools to respond to changing threats. But the CFAA has not been amended since 2008, and the intervening years have again created the need for the enactment of modest, incremental changes. The Administration's May 2011 legislative proposal proposed revisions to keep Federal criminal law up to date. We continue to support changes like these that will keep up with rapidly evolving technologies and uses.

In addition, our investigations of those responsible for creating and using botnets and our efforts to disrupt botnets rely substantially on the availability of legal investigative process pursuant to the Electronic Communications Privacy Act ("ECPA"). ECPA governs the Department's access to much of the electronic evidence necessary to investigate botnets, hold perpetrators accountable, and develop methods to free unsuspecting victims. It is essential to the success of our anti-botnet initiatives, and to our efforts against cybercrime as a whole, that the government maintain the ability to obtain relevant electronic evidence in a responsible, timely and effective manner.

Selling Access to Botnets

In the years since 2011, experience has revealed additional shortcomings in the criminal law. For example, while botnets can be used for various nefarious purposes, including theft of personal or financial information, the dissemination of spam, and DDOS attacks, the creators and operators of botnets do not always commit those crimes themselves. Frequently they sell, or even rent, access to the infected computers to others. The CFAA does not clearly cover such trafficking in access to botnets, even though trafficking in infected computers is clearly illegitimate, and can be essential to furthering other criminal activity. We thus propose that section 1030(a)(6) of the CFAA be amended to cover trafficking in access to botnets.

In addition, section 1030(a)(6) presently requires proof of an intent to commit a financial fraud. Such intent is often difficult—if not impossible—to prove because the traffickers of unauthorized access to computers often have a wrongful purpose other than the commission of fraud. Indeed, sometimes they may not know or care why their customers are seeking unauthorized access to other people's computers. This reality has made it more challenging in many cases for our prosecutors to identify a provable offense, even when we can establish beyond a reasonable doubt that individuals are selling access to thousands of infected computers. We therefore recommend that Congress amend section 1030(a)(6) of the CFAA to address this shortcoming. .

Enhancing Judicial Authority to Disrupt Botnets and other Malware

Under current law, two federal statutes, 18 U.S.C. §§ 1345 & 2521, give the Attorney General the authority to bring civil suits against defendants who are engaged in or "about to" engage in wiretapping or the violation of specified fraud crimes.[1] *See* 18

[1] The specified fraud crimes include those listed in Title 18, Chapter 65 (mail fraud, wire fraud, bank fraud, and health care fraud), section 287 (fraudulent claims), section 1001

U.S.C. §§ 1345(a), 2521. The court is then empowered to enjoin the violation, "or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought." 18 U.S.C. § 1345(b); *see also* 18 U.S.C. § 2521. Due process is ensured by the balancing test applied by the court to determine whether an injunction is appropriate and by the applicable Federal Rules of Civil Procedure.

These authorities played a prominent role in the Department's successful disruptions of the Coreflood botnet in 2011 and the Gameover Zeus botnet in 2014. These botnets collected online financial account information as it was transmitted from infected computers, thus violating the Wiretap Act, and the criminals used their access to steal from victims' bank accounts, which constitutes wire and bank fraud. Because these botnets violated statutes against fraud and wiretapping, courts were authorized to issue orders under sections 1345 and 2521 that permitted the United States to take corrective action necessary to disrupt them.

No analogous statutory authority exists, however, for violations of the CFAA that do not involve fraud or the interception of communications. As a result, the law does not provide a clear statutory remedy for the government to use against botnets or other types of malware that criminals employ for other purposes, such as DDOS attacks. Similar to frauds and illegal wiretaps, these types of computer hacking—which are prohibited under section 1030—present serious threats that can cause severe and continuing damage as long as they persist. We would welcome the opportunity to work with the Committee to ensure that the law appropriately addresses this challenge.

Criminalizing the Overseas Sale of Stolen U.S. Financial Information

To ensure that we can take action when cyber criminals acting overseas steal data from U.S. financial institutions, we also recommend a modification to what is known as the access device fraud statute, 18 U.S.C. § 1029. One of the most common motivations for criminal hacking is to obtain financial information. The access device fraud statute

(false statements to government officers), and conspiracies to commit these offenses. *See* 18 U.S.C. § 1345(a)(1).

proscribes the unlawful possession and use of "access devices," such as credit card numbers and devices such as credit card embossing machines. Not only do lone individuals commit this crime, but, more and more, organized criminal enterprises have formed to commit such intrusions and to exploit the stolen data through fraud.

The Department of Justice recommends that the statute be expanded to enable prosecution of offenders based in foreign countries who directly and significantly harm United States financial institutions and citizens. Currently, a criminal who trades in credit card information issued by a U.S. financial institution, but who otherwise does not take one of certain enumerated actions within the jurisdiction of the United States, cannot be prosecuted under section 1029(a)(3). Such scenarios are not merely hypothetical. United States law enforcement agencies have identified foreign-based individuals selling vast quantities of credit card numbers issued by U.S. financial institutions where there is no evidence that those criminals took a specific step within the United States to traffic in the data. The United States has a compelling interest in prosecuting such individuals given the harm to U.S. financial institutions and American citizens, and the statute should be revised to cover this sort of criminal conduct.

Enhancing Resources to Combat Botnets and other Cyber Threats

This last May, the Department submitted to Congress a multiyear cyber threat strategic plan. The report identified six strategic initiatives:

- Ensure that all of DOJ's investigators and attorneys receive training on cybercrime and digital evidence.
- Increase the number of digital forensic experts and the capacity of available digital forensic hardware.
- Enhance DOJ's expertise in addressing complex cyber threats.
- Improve information sharing efforts with the private sector.
- Expand and strengthen relationships with international law enforcement and criminal justice partners on cybercrime to enhance the sharing of electronic evidence.

- Enhance capacity in the area of cyber policy development and associated legislative work.

The plan repeatedly highlighted the disruption of botnets as a key priority. In order to properly address the threat of botnets and other cybercrimes, components across the Department, such as CCIPS, NSD, and the United States Attorneys' Offices, need additional resources.

The Department confronts an increasing demand for its anti-cybercrime expertise. CCIPS, for example, conducts its own prosecutions, receives requests for consultation of its attorneys or digital investigative analysts, provides advice to law enforcement agencies, engages with the private sector regarding the implementation of investigative authorities, and delivers domesic and international training. This escalation in activity is due in part to the ever-expanding nature of the cyber threat. Prosecutorial needs have also resulted from the expansion of investigative efforts, as the FBI has increased its resources in support of the Next Generation Cyber Initiative to enhance the technical capabilities of investigative personnel, increase cyber investigations, and improve cyber collection and analysis

The Department would like to thank the Senate for its continued support of our national security-related cyber efforts, including fiscal year 2014 funding increases that are allowing the Department to hire more than a dozen additional national security cyber professionals, including attorneys, in furtherance of our efforts to combat cyber-based terrorism and nation state-sponsored cyber intrusions. Just this summer, thanks in part to your support, those efforts yielded historic results, with the indictment of five members of the Chinese military on charges of cyber-based economic espionage. Cyber threats to the national security continue to evolve, and to outpace our growth, but the Department is committed to following the facts and evidence where they lead to detect, deter, and disrupt them. We look forward to continuing to work with you on this front.

Conclusion

I very much appreciate the opportunity to discuss with you the Department's efforts to combat botnets. We are committed to using all available tools to disrupt these networks and bring perpetrators to justice, as we seek to protect Americans' security, privacy, and property.

Thank you for the opportunity to discuss the Department's work in this area, and I look forward to answering any questions you might have.

Department of Justice

STATEMENT OF

JOSEPH DEMAREST
ASSISTANT DIRECTOR
CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SUBCOMMITTEE ON CRIME AND TERRORISM
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ENTITLED

"TAKING DOWN BOTNETS: PUBLIC AND PRIVATE EFFORTS TO DISRUPT AND DISMANTLE CYBERCRIMINAL NETWORKS"

PRESENTED

JULY 15, 2014

Statement of
Joseph Demarest
Assistant Director
Cyber Division
Federal Bureau of Investigation

Before the
Committee on the Judiciary
Subcommittee on Crime and Terrorism
United States Senate

At a Hearing Entitled
"Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks"

Presented
July 15, 2014

Good morning Senator Whitehouse. I thank you for holding this hearing today, and I look forward to discussing the progress the FBI has made on campaigns to disrupt and disable significant botnets.

As you well know, we face cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and terrorists. They seek our state secrets, our trade secrets, our technology, and our ideas – things of incredible value to all of us. They may seek to strike our critical infrastructure and our economy. The threat is so dire that cyber security has topped the Director of National Intelligence list of global threats for the second consecutive year.

Cyber criminal threats post very real risks to the economic security and privacy of the United States and its citizens. The use of botnets is on the rise. Industry experts estimate that botnets attacks have resulted in the overall loss of millions of dollars from financial institutions and other major U.S. businesses. They also affect universities, hospitals, defense contractors, government, and even private citizens.The "weapons" of a cyber criminal are tools, like botnets, which are created with malicious software that is readily available for purchase on the Internet. Criminals distribute malicious software, also known as malware, that can turn a computer into a "bot." When this occurs, a computer can perform automated tasks over the Internet, without any direction from its rightful user. A network of these infected computers—numbering in the hundreds of thousands or even millions—is called a botnet (robot network), and each computer becomes connected to a command-and-control server operated by the criminal.

Once the botnet is in place, it can be used in distributed denial of service (DDoS) attacks, proxy and spam services, malware distribution, and other organized criminal activity. Botnets can also be used for covert intelligence collection, and terrorists or state-sponsored actors could use a botnet to attack Internet-connected critical infrastructure. And, they can be used as weapons in ideology campaigns against their target to instigate fear, intimidation, or public embarrassment.

A botnet typically operates without obvious visible evidence and can remain operational for years.

Our personal computers can become part of a botnet—it only takes one wrong click for a home user to download malicious code. For example, you might get an unsolicited e-mail promoting a dating website or a work-at-home arrangement or an e-mail that appears to come from your bank containing a seemingly harmless link. You could be sent a link by a friend asking you to view a great video, which was actually sent because your friend's computer is already infected. You could see a link on a webpage that seems to be soliciting donations for a recent tragedy. And you might even visit a fraudulent website—or a legitimate one that's been compromised—and download video, pictures, or a document containing malicious code.

Once the malware is on your computer, it's hard to detect. In addition to your computer being commanded to link up with other compromised computers to facilitate criminal activity, the bot can also collect and send out your personal identifiable information—like credit card numbers, banking information, and passwords—to the criminals running it. Those criminals will take advantage of the information themselves or offer it for sale on cyber criminal forums.

The impact of this global cyber threat has been significant. According to industry estimates, botnets have caused over $9 billion dollars in losses to U.S. victims and over $110 billion in losses globally. Approximately 500 million computers are infected globally each year, translating into 18 victims per second.

The FBI, with its law enforcement and private sector partners, has had success in taking down a number of large botnets. But our work is never done, and by combining the resources of government and the private sector, and with the support of the public, we will continue to improve cyber security by identifying and catching those who threaten it.

FBI's Cyber Criminal Strategy

Due to the complicated nature of today's cyber criminal threat, the FBI has developed a strategy to systematically identify cyber criminal enterprises and individuals involved in the development, distribution, facilitation, and support of complex criminal schemes impacting U.S. systems. This complete strategy involves a holistic look at the entire cyber underground ecosystem and all facilitators of a computer intrusion.

The FBI's overall goal is to remove, reduce, and prevent cyber crime by attacking the threat through the identification of the most significant cyber criminal actors. Our success can only be attained through coordination of our overall cyber criminal strategy amongst all FBI Cyber Division's existing and emerging entities.

Just last month, the FBI Cyber Division evolved to create a threat-model approach to address the most significant domestic and international cyber threats. The FBI cyber criminal strategy consists of the newly established Major Cyber Crimes Unit, which serves as the primary headquarters unit addressing the cyber criminal threat by providing strategic and field office operational support; the Cyber Initiative and Resource Fusion Unit (CIRFU) which supports the National Cyber Forensics and Training Alliance (NCFTA) and is comprised of representatives from industry, academia, and the FBI; and the Internet Crime Complaint Center (IC3) which has a vital role in the identification of cyber fraud-related threats. All of these entities work together to enhance and support field office operations by developing and maintaining long-term strategies to infiltrate cyber criminal networks, provide tactical support, and develop intelligence collection opportunities against predicated targets.

The FBI cyber criminal strategy also includes working closely with our international partners to develop a holistic assessment of the threat posed by cyber criminals and organizations to partner countries. Through this collaborative process, the FBI hopes to launch aggressive and comprehensive mitigation strategies through joint investigations and operational partnerships with law enforcement partners, private industry, and academia.

These important components of the FBI cyber criminal strategy coordinate efforts with the National Cyber Investigative Joint Task Force (NCIJTF), which is intended to be the focal point for all U.S. government agencies to coordinate, integrate, and share domestic cyber threat information specific to national security investigations.

FBI Efforts to Combat Botnets

Through the NCIJTF, and in alliance with its U.S. government (USG) partners, international partners, and private sector stakeholders, the FBI has worked collaboratively in developing a multi-pronged effort aimed at defeating the world's most dangerous botnets.

Over the past several years, the FBI's efforts to combat these significant cyber threats have caused the disruption and dismantlement of numerous botnets including Butterfly Bot, Rove Digital, Coreflood, ZeroAccess, and Gameover Zeus, resulting in numerous arrests, extraditions, and convictions.

Operation Clean Slate

In April 2013, the FBI initiated an aggressive approach to disrupt and dismantle the most significant botnets threatening the U.S. economy and our national security. This initiative, named Operation Clean Slate, is spearheaded by the FBI's NCIJTF. It is a comprehensive, public/private effort engineered to eliminate the most significant botnets jeopardizing U.S. interests by targeting the criminal coders who create them. This initiative incorporates all facets of the USG, international partners, major Internet service providers, the U.S financial sector, and other private sector cyber stakeholders.

Operation Clean Slate has three objectives: (1) to degrade or disrupt the actor's ability to exfiltrate sensitive information from U.S. networks through arrests, by deploying a technical solution to interrupt the botnet, and by working with private sector partners to update security software that detects and damages the bot's malware; (2) to increase the actor's cost of business by causing wasted time debugging failures, or forcing an actor to write new code for new botnet attacks; and (3) to seed uncertainty in the actor's cyber activity by causing concern about potential or actual law enforcement action.

The FBI Cyber Division ranked the Citadel Botnet as the highest priority under the Operation Clean Slate initiative. In June 2013, the FBI, in coordination with its partners, disrupted the Citadel Botnet which had facilitated unauthorized access to computers of individuals and financial institutions to steal online banking credentials, credit card information, and other personally identifiable information. Citadel was responsible for the loss of over a half billion dollars. Over 1,000 Citadel domains were seized, accounting for more than 11 million victim computers worldwide.

In separate but coordinated operations, the FBI, Microsoft, and financial services industry leaders successfully disrupted more than 1,000 botnets built on Citadel malware in a massive global cyber crime operation that is estimated by the financial services industry to have been responsible for over half a billion dollars in financial fraud. Microsoft exercised its independent civil authorities in this matter. The company then coordinated with the FBI and other private parties. The FBI provided information to foreign law enforcement counterparts so that they could also take voluntary action on botnet infrastructure located outside of the United States. The FBI also obtained and served court-authorized search warrants domestically related to the botnets.

Building on the success of the disruption of Citadel, in December 2013, the FBI and Europol, together with Microsoft and other industry partners, disrupted the ZeroAccess botnet. ZeroAccess was responsible for infecting more than two million computers, specifically targeting search results on Google, Bing, and Yahoo search engines and is estimated to have cost online advertisers $2.7 million each month.

Recent Successes

Other recent FBI successes in combating the botnet threat include domestic and international investigative efforts which have resulted in indictments, arrests, and extraditions. Examples include:

- In April 2011, the FBI executed criminal seizure warrants to disable an international botnet consisting of hundreds of thousands of computers infected with a malicious software program known as Coreflood. Coreflood allowed infected computers to be controlled remotely for the purpose of stealing private personal and financial information from unsuspecting computer users, including users on corporate computer networks, and used that information to steal funds.

- In November 2011, a two-year FBI investigation called Operation Ghost Click resulted in the dismantlement of an international cyber ring that infected millions of computers worldwide with a virus that enabled the thieves to manipulate the multi-billion-dollar Internet advertising industry. In November 2013, three Estonian nationals were extradited to the United States to face charges related these crimes.

- In December 2012, the FBI disrupted an international organized cyber crime ring related to Butterfly Botnet,which stole computer users' credit card, bank account, and other personally identifiable information. Butterfly Botnet compromised more than 11 million computer systems and resulted in over $850 million in losses. The FBI, along with international law enforcement partners, executed numerous search warrants, conducted interviews, and arrested 10 individuals from Bosnia and Herzegovina, Croatia, Macedonia, New Zealand, Peru, the United Kingdom, and the United States.

- In April 2014, the FBI's investigative efforts resulted in the indictments of nine alleged members of a wide-ranging racketeering enterprise and conspiracy who infected thousands of business computers with malicious software known as "Zeus," which is malware that captured passwords, account numbers, and other information necessary to log into online banking accounts. The conspirators allegedly used the information captured by "Zeus" to steal millions of dollars from account-holding victims' bank accounts.

- In May 2014, the FBI announced the indictments of a Swedish national and a U.S. citizen believed to be the co-developers of a particularly insidious computer malware known as Blackshades. This software was sold and distributed to thousands of people in more than 100 countries and has been used to infect more than half a million computers worldwide. Also charged and arrested in the United States was an individual who helped market and sell the malware, and two Blackshades users who bought the malware and then unleashed it upon unsuspecting computer users, surreptitiously installing it on their hardware. At least 40 FBI field offices conducted approximately 100 interviews, executed more than 100 e-mail and physical search warrants, and seized more than 1,900 domains used by Blackshades users to control victims' computers, and at least 18 other countries were involved in executing more than 90 arrests and more than 300 searches.

- In June 2014, the FBI announced a multinational effort to disrupt the GameOver Zeus botnet, the most sophisticated botnet that the FBI and its allies had ever attempted to disrupt. GameOver Zeus is believed to be responsible for the theft of millions of dollars from businesses and consumers in the U.S. and around the world. This effort to disrupt it involved impressive cooperation with the private sector and international law enforcement. GameOver Zeus is an extremely sophisticated type of malware designed specifically to steal banking and other credentials from the computers it infects. In the case of GameOver Zeus, its primary purpose is to capture banking credentials from infected computers, then use those credentials to initiate or re-direct wire transfers to accounts overseas that are controlled by the criminals. Losses attributable to GameOver Zeus are estimated to be more than $100 million.

Way Forward

The FBI is proud of these successes, but we recognize that we must constantly strive to be more efficient and effective. Just as our adversaries continue to evolve, so, too, must the FBI. We live in a time of sophisticated cyber criminal threats - threats that most often impact our private citizens.

Much like with the FBI's other investigative priorities where we focus on the impacting the leaders of a criminal enterprise or terrorist organization, we are focusing on the major cyber actors behind the botnets. The FBI must also continue to develop and deploy creative solutions in order to defeat today's complex cyber threat actors. This includes R&D addressing how to identify and shut down botnets faster than they are created and used. We also strive to build better relationships in order to overcome the obstacles that prevent us from collaborating and sharing information.

We remain focused on defending the United States against these threats, and we welcome opportunities like the one today to discuss these efforts. We are grateful for the Committee's support, and we look forward to working with you as we continue to forge aggressive campaigns against botnets.

Written Testimony of
Richard Domingues Boscovich
Assistant General Counsel, Digital Crimes Unit
Microsoft Corporation

Before the
Senate Committee on the Judiciary
Subcommittee on Crime and Terrorism

Taking Down Botnets: Public and Private Efforts to
Disrupt and Dismantle Cybercriminal Networks

July 15, 2014

Chairman Whitehouse, Ranking Member Graham, and members of the Subcommittee, thank you for the opportunity to discuss Microsoft Corporation's approach to detecting and fighting botnets. We also thank you for your leadership in focusing attention to this complicated, but important topic. My name is Richard Domingues Boscovich, and I am Assistant General Counsel in Microsoft's Digital Crimes Unit.

Before joining Microsoft in 2008, I was an Assistant United States Attorney in the Southern District of Florida for 17 years, and served as director of that District's Computer Hacking and Intellectual Property Unit. I have witnessed the evolution of cybercrime since the infancy of the Internet, and botnets are among the most malicious online threats that I have ever seen. Botnets are groups of computers remotely controlled by hackers without their owners' knowledge or consent. Botnets infect millions of computers at a time and enable criminal enterprises to invade the privacy of unsuspecting victims and steal their identities and money.

To understand the devastating impact of botnets, we can look at how they affected one victim. Consider Eunice Power, a chef in the United Kingdom, who turned on her laptop one day to find a warning that she could not access her files unless she paid ransom to cybercriminals within 72 hours. When she failed to meet the deadline, all of her photos, financial account information, and other data were permanently deleted. As she later told a reporter, "[i]f someone had robbed my house it would have been easier."

Indeed, botnets conduct the digital equivalent of home invasions, on a massive scale. Botnet operators quietly hijack webcams to spy on people in their homes, and later sell explicit photographs of the unsuspecting victims on the black market. They use malicious software to log every keystroke that users enter on their computers—including credit card numbers, Social Security numbers, work documents, and personal emails. They send deceptive emails designed to appear as though they were sent by banks that convince consumers to disclose financial account information.

Botnets are exponentially more damaging—and efficient—than traditional computer viruses. Because a botnet gets stronger as it infects more computers, a single botnet allows a cybercriminal to commit tens of billions of illegal acts in a single day. For example, the Citadel family of botnets caused more than a half-billion dollars in economic damage worldwide before Microsoft helped disrupt it last year.

For more than a decade, Microsoft has partnered with other companies and global law enforcement agencies to battle such malicious cybercriminals. I am happy to be joined today by representatives of Symantec and the FBI, who are among our key partners in this battle and who have helped us disrupt some of the world's most malicious botnet operations. Today, I will tell you about Microsoft's approach to combatting botnets by disrupting their economic infrastructure, the legal and technical tactics that we use to identify and take down botnets, our approach to protecting consumer privacy while fighting botnets, the outstanding results that have come from our public-private partnerships, and lessons learned along the way.

Botnet Prevention Requires Cooperation between Law Enforcement and the Private Sector

We do not—and cannot—fight botnets alone. As the title of this hearing suggests, fighting botnets requires efforts from both the private *and* public sector. We routinely work with other companies and domestic and international law enforcement agencies to dismantle botnets that have caused billions of dollars in worldwide economic damage. In addition to the FBI and Symantec, we regularly work with a wide range of academics from institutions that include the Universities of California at Berkeley, Santa Cruz, and San Diego as well as the University of Washington. Industry partners include CSIS.DK, FireEye, F-Secure, Kaspersky, and Kyryus. Our joint efforts demonstrate that public-private partnerships are highly effective at combatting cybercrime. Moreover, we believe that public-private partnerships are essential to addressing the increasingly complex problems presented by cybercrime; no single individual or entity can tackle these problems alone.

To that end, we monitor evolving cybercrime threats and work closely with law enforcement on a number of initiatives to help devise and execute strategies that disrupt cybercrime threats targeting Microsoft technology, people, businesses, and critical infrastructure. Microsoft also supports governments and law enforcement by providing them with technical training, investigative and forensic assistance, and the continued development of new tools to combat cybercrime. Once Microsoft discovers a botnet and disrupts its network infrastructure, it works with Internet Service Providers (ISPs) and Computer Emergency Response Teams (CERTs) to rescue and clean computers from the control of the botnets.

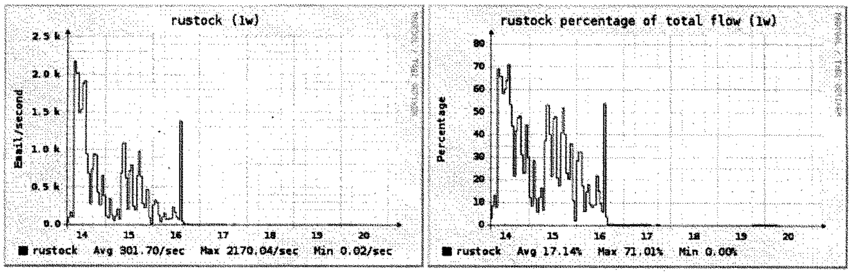
Microsoft's anti-botnet program uses the civil litigation system. We believe that civil litigation remedies, including injunctions, are appropriate and effective tools for stopping the harms caused by those who use criminal botnets to violate commercial and intellectual property laws. We also believe there is a vital role for law enforcement in this fight. While Microsoft clearly does not have access to criminal enforcement tools, we work to partner with law enforcement wherever appropriate. We also try to carefully structure our operations to ensure that we complement the efforts of law enforcement and avoid unintentionally interfering with criminal investigations or prosecutions.

Our public-private partnerships have led to significant successes. We helped to disrupt 11 botnets tied to criminal organizations committing consumer, financial, and advertising fraud, which led to the disruption of widespread criminal enterprises and the cleanup of millions of infected computers.

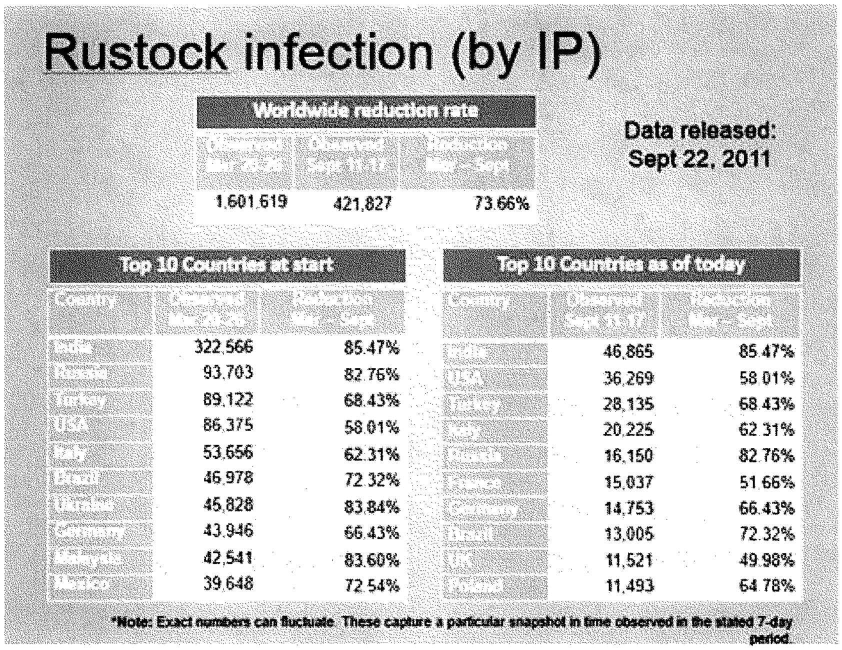
Consider the March 17, 2011 shut-down of the Rustock botnet, which at one time was responsible for approximately half of the world's spam. Microsoft worked with Pfizer, whose drugs often were the subject of Rustock spam, security experts at the University of Washington, and other law enforcement and governmental authorities, including Dutch law enforcement agencies, to dismantle this global botnet. Alex Lanstein, Senior Engineer at network security provider FireEye, said that Microsoft "did a public service" by coordinating the legal efforts to obtain control of the botnet.

The following chart shows the change in spam flow from the Rustock botnet during the week of the shut-down:

Week of Rustock Shutdown



Source: http://cbl.abuseat.org/rustock.html (visited July 11, 2014).



Rustock infection (by IP)

Data released:
Sept 22, 2011

Worldwide reduction rate		
Observed Mar 20-26	Observed Sept 11-17	Reduction Mar – Sept
1,601,619	421,827	73.66%

Top 10 Countries at start		
Country	Observed Mar 20-26	Reduction Mar – Sept
India	322,566	85.47%
Russia	93,703	82.76%
Turkey	89,122	68.43%
USA	86,375	58.01%
Italy	53,656	62.31%
Brazil	46,978	72.32%
Ukraine	45,828	83.84%
Germany	43,946	66.43%
Malaysia	42,541	83.60%
Mexico	39,648	72.54%

Top 10 Countries as of today		
Country	Observed Sept 11-17	Reduction Mar – Sept
India	46,865	85.47%
USA	36,269	58.01%
Turkey	28,135	68.43%
Italy	20,225	62.31%
Russia	16,150	82.76%
France	15,037	51.66%
Germany	14,753	66.43%
Brazil	13,005	72.32%
UK	11,521	49.98%
Poland	11,493	64.78%

*Note: Exact numbers can fluctuate. These capture a particular snapshot in time observed in the stated 7-day period.

Source: Microsoft

Similarly, last month, Microsoft and the FBI worked together to disrupt the GameOver Zeus botnet, which stole passwords via peer-to-peer technology, making it particularly difficult to track. Microsoft provided the FBI with technical analysis of the peer-to-peer network and developed a cleaning solution, as the FBI and Justice Department took control of the domains and filed criminal charges against the Russian hacker who led the botnet. As one reporter observed in an article about the disruption, "the biggest champion of the day may be collaboration between the feds and the private sector." It was this particular botnet that led to the theft of personal information that I described earlier in my testimony.

Disrupting Botnets' Economic Infrastructure

Microsoft's philosophy to fighting botnets is simple: we aim for their wallets. We disrupt botnets by undermining cybercriminals' ability to profit from malicious attacks.

At bottom, cybercriminals operate botnets to make money. Botnets are businesses, albeit illegal ones. Botnets are particularly attractive tools for criminals because they are cheap and effective. They have a relatively low cost of entry, the marginal cost to maintain them is low, and the potential profits grow exponentially as more computers are infected.

Microsoft has seen botnets take many forms and use a wide range of tools. But a common theme among all of them is the desire to generate a profit for the botnet operators. Consider the "business models" of the most malicious botnets:

- **Zeus** botnets, a family of financial botnets that were responsible for identity theft, caused more than $70 million in financial losses, and infected more than 13 million PCs worldwide.

- **Bamital** botnet, which hijacked people's search results, taking them to potentially dangerous websites that could install malware, steal personal information, or fraudulently charge businesses for "clicks" on online advertisements. More than 8 million computers had been attacked by Bamital in the two years prior to its takedown.

- **Nitol** botnet, which used more than 500 different strains of malware to potentially target millions of innocent people and steal their personal information, including financial account data. It was discovered as part of a Microsoft study on unsecured supply chains, which found that 20 percent of PCs purchased for analysis in China from unsecure supply chains were infected with malware.

- **Rustock** botnet, which was reported to be among the world's largest "spambots," could send up to 30 billion spam email messages per day. It infected nearly 2.5 million computers worldwide.

I am proud to report that Microsoft, in partnership with other companies and law enforcement agencies worldwide, has disrupted all of these botnets—and others—and as a result has dramatically increased their costs of "doing business." By disrupting their infrastructure, we impact the bottom-line cost-benefit equation for cybercriminals. In doing so, we seek not only to protect users from the existing botnets, but to alter the financial analysis for criminals to the point that they are discouraged from establishing new botnets.

Protecting Consumers

Microsoft draws on our deep technical and legal expertise to develop carefully planned and executed operations that disrupt botnets pursuant to court-approved procedures.

Microsoft's Digital Crimes Unit ("DCU") is a team of more than 100 technical, legal and business experts that uses creative techniques and Microsoft technology to fight cybercrime and improve cybersecurity. The DCU proactively helps Microsoft customers stay ahead of new and evolving threats and challenges. Through robust partnerships and a recognition that no one company can fight cybercrime alone, DCU plays offense against online threats.

Microsoft's work in this area dates back more than a decade. In 2003, Microsoft formed a joint legal and technical team to address cybercrime, known as the Internet Safety and Enforcement Team ("ISET"), as part of Microsoft's Trustworthy Computing initiative. In 2008, ISET evolved to become the DCU, to better align with how Microsoft was tackling the evolution of cybercrime. Last year, Microsoft opened its Cybercrime Center, combining our legal and technical expertise with cutting-edge tools and technology to mark a new era in the fight against cybercrime.

The DCU uses a combination of legal and technical tactics to help fight cybercrime. In general terms, Microsoft asks a court for permission to sever the command-and-control structures of the most destructive botnets, breaking communication lines to either the domains or Internet protocol (IP) addresses that cybercriminals use to control the botnet.

Once the court grants permission and Microsoft severs the connection between a cybercriminal and an infected computer, traffic generated by infected computers is either disabled or routed to domains controlled by Microsoft. This process, known as "sinkholing," helps Microsoft collect valuable evidence and intelligence used to help notify victims that their computers are infected, as well as clean computers to remove the malicious software. These disruptions significantly impact cybercriminals' operations and infrastructure, assists victims in regaining control of infected computers and furthers investigations against cybercriminals responsible for the threat. As we execute these court orders, we work hard to avoid disrupting legitimate Internet traffic and, where necessary, we will take steps during or after implementation of a court order to achieve that goal.

As one example, in May 2013, Microsoft worked closely with the FBI to disrupt a massive cybercrime ring associated with the Citadel botnet. As part of those efforts, Microsoft asked the United States District Court in the Western District of North Carolina to grant an emergency temporary restraining order, seizure order, and an order to show cause for preliminary injunction, to help disrupt the botnet. Microsoft argued the botnet violated a number of state and federal laws, including the Computer Fraud and Abuse Act (18 U.S.C. §1030), the CAN-SPAM Act (15 U.S.C. §7704), the Electronic Communications Privacy Act (18 U.S.C. §2701), the Lanham Act (15 U.S.C. §§ 1114), the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962), and the North Carolina Computer Trespass law (N.C. Gen. Stat. §14-458), as well as the common law torts of conversion, unjust enrichment, and nuisance.

Microsoft supported this request with evidence of how the Citadel botnet worked, and of the harm it caused to infected computers. In authorizing that request, the court: (1) enjoined the operators of the Citadel botnets from continuing to operate those botnets, (2) required domain registries to redirect a list of currently-registered domain names to secure servers, (3) required domain registries to transfer a list of currently-unregistered domain names into Microsoft's control, so they could not be used for the botnet, (4) required ISPs to log all attempts to communicate with specific IP addresses associated with the botnet, and provide documentation to Microsoft showing the persons who operate those IP addresses, (5) authorized Microsoft to cause all Citadel-infected computers attempting to connect to Citadel servers to connect instead to Microsoft servers, and install a curative file that stops the harmful acts of the botnet, and (6) authorized Microsoft to alert end-users when an infected computer attempted to connect to any Internet site, and direct them to a Microsoft or antivirus site to download curative files.

The court's order authorized Microsoft to disrupt more than 1,400 Citadel botnets that were responsible for more than half a billion dollars in losses to persons and businesses worldwide. At the same time, the FBI took coordinated separate steps related to the investigation, marking the first time that law enforcement and the private sector worked together in this way to execute a civil seizure warrant as part of a botnet disruption operation.

Transparency and Privacy are Core Values of Our Anti-Botnet Operations

Obtaining control of botnet domains is only the first step in preventing the spread of botnets and remediating the harm that they have caused. Once Microsoft receives information about a botnet, Microsoft disseminates this data to partners so that infected computers can be cleaned. Microsoft has worked in cooperation with numerous ISPs and CERTs around the world to help notify affected customers and connect them with tools to clean their devices.

Broad distribution of this information is crucial to remediating the harm that the botnets have caused, and preventing the botnets from growing. Microsoft makes information about botnets available to ISPs and CERTs through our Cyber Threat Intelligence Program ("C-TIP"). That service allows ISPs and CERTs to receive updated threat data related to infected computers in their specific country or network approximately every 30 seconds.

Last year, Microsoft and the Secretary of State of Telecommunications and Information Society of Spain announced an important agreement under which the Spanish CERT, INTECO, became one of the first organizations to receive data from the C-TIP cloud service. All the information is uploaded directly to each organization's private cloud through Windows Azure. INTECO joined the Luxembourg CERTs, CIRCL and gov CERT, as early adopters of this program. By participating in this system, organizations have almost instant access to threat data generated from previous as well as future operations conducted by the Microsoft Active Response for Security program.

The cloud-based C-TIP program represents an evolution in such information-sharing. In 2010, the original C-TIP program began sending regular emails to participating ISPs and CERTs with threat intelligence for their customers and regions. As of 2013, 44 organizations in 38 countries received these threat intelligence emails, and momentum is building for the program. The new cloud-based program dramatically increases our ability to clean computers and help us keep up with the fast-paced and ever-changing cybercrime landscape. It also gives us another advantage: cybercriminals rely on infected computers to exponentially leverage their ability to commit their crimes. If we are able to take those resources away from them, they will have to spend time and money trying to find new victims, thereby making these criminal enterprises less lucrative and appealing in the first place.

Privacy also is a fundamental value in Microsoft's anti-botnet operations. When we execute a botnet operation, we operate within the bounds of the court order. We never look at the underlying communications sent by infected computers. Instead, Microsoft only accesses the IP address used by the infected computer, so that we can help the ISPs and CERTs notify the user of the infection and assist in the remediation. We work with ISPs so they can alert their customers directly.

In addition, Microsoft makes resources available online so that consumers can help avoid becoming victims in the first place or clean infected computers. Individuals and businesses worldwide should exercise safe practices, such as running up-to-date, legitimate software. Additionally, people should use protections like firewalls and anti-virus/anti-malware programs and exercise caution when surfing the internet or clicking on ads or email attachments, as they could be malicious. More information on how to stay safe online can be found at http://www.microsoft.com/protect. People worried that their computers might be infected with malware, can obtain free information and malware cleaning tools from Microsoft at: http://support.microsoft.com/botnets.

Improving Laws to Battle Botnets

Microsoft welcomes the Subcommittee's strong interest in this growing threat, and appreciates your efforts to provide us with more tools to fight botnets. In particular, Microsoft believes that changes to two existing laws could go a long way toward battling botnets.

First, Microsoft supports amending the Computer Fraud and Abuse Act (CFAA), which long has allowed the government and private individuals to hold computer hackers responsible for unauthorized access to computers. Unfortunately, the law was enacted in 1986, long before we envisioned the command structure of botnets. In many cases, the botnet operator develops a system that enables *others* to conduct the actual hacking. Although some botnet operators have been convicted under the CFAA, we agree with the Department of Justice that the statute would be a more effective tool if it explicitly covered trafficking in access to botnets. Microsoft also agrees with the Department of Justice that Congress should amend Section 1030(a)(6) of the CFAA to eliminate the requirement of proof of intent to defraud, which in some botnet cases is difficult to demonstrate.

Finally, Microsoft agrees with the Department of Justice that Congress should amend the Access Device Fraud statute, which allows prosecutors to bring charges against the perpetrators of phishing and other credit card fraud schemes. The amendment should apply the statute to offenders in foreign countries who directly and significantly harm individuals and financial institutions in the United States. This change would provide both additional methods to disrupt phishing botnets that originate in other countries.

✧ ✧ ✧

In summary, Microsoft's participation in public-private partnerships has resulted in the disruption and shut-down of some of the most malicious threats to public trust and security on the Internet. But our work is never done, as cybercriminals develop new and more sophisticated methods to profit from the online chaos that they create. The criminals will continue to evolve and develop more sophisticated tools. So will Microsoft. We remain firmly committed to working with other companies and law enforcement to disrupt botnets and make the Internet a more trusted and secure environment for everyone.

Symantec™

Prepared Testimony and
Statement for the Record of

Cheri F. McGuire
Vice President, Global Government Affairs & Cybersecurity Policy
Symantec Corporation

Hearing on

"Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks"

Before the

United States Senate
Committee on the Judiciary
Subcommittee on Crime and Terrorism

July 15, 2014

226 Dirksen Senate Office Building

Chairman Whitehouse, Ranking Member Graham, and distinguished members of the Subcommittee, thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Cheri McGuire and I am the Vice President for Global Government Affairs and Cybersecurity Policy at Symantec. I am responsible for Symantec's global public policy agenda and government engagement strategy, which includes cybersecurity, data integrity, critical infrastructure protection (CIP), and privacy. I lead a team of professionals spanning the U.S., Canada, Europe, Asia, and Latin America, and represent the company in key policy organizations. In this capacity, I work extensively with industry and government organizations, including serving from 2010 to 2012 as Chair of the Information Technology Sector Coordinating Council (IT SCC) – one of 16 critical sectors identified by the President and the US Department of Homeland Security (DHS) to partner with the government on CIP and cybersecurity. I also serve as a board member of the Information Technology Industry Council (ITI), the US Information Technology Office (USITO) in China, and the National Cyber Security Alliance (NCSA). I am also a past board member of the IT Information Sharing and Analysis Center (IT-ISAC). Previously, I served in various positions at DHS, including as head of the National Cyber Security Division and US Computer Emergency Readiness Team (US-CERT).

Symantec protects much of the world's information, and is a global leader in security, backup and availability solutions. We are the largest security software company in the world, with over 32 years of experience developing Internet security technology and helping consumers, businesses and governments secure and manage their information and identities. Our products and services protect people's information and their privacy across platforms – from the smallest mobile device, to the enterprise data center, to cloud-based systems. We have established some of the most comprehensive sources of Internet threat data in the world through our Global Intelligence Network, which is comprised of millions of attack sensors recording thousands of events per second, and we maintain 10 Security Response Centers around the globe. In addition, we process billions of e-mail messages and web requests across our 14 global data centers. All of these resources allow us to capture worldwide security data that give our analysts a unique view of the entire Internet threat landscape.

The cyber headlines of the past year have focused on massive data breaches and cyber espionage. While these are critically important issues, botnets – or networks of infected computers – are the foundation of the cyber-criminal ecosystem, and I am pleased that you again are focusing attention on how industry and government are working to disrupt them. In my testimony today, I will discuss:

- Types of botnets we are seeing and what we may see in the future;
- Efforts to disrupt botnets;
- Assistance for victims of botnets and combating cybercrime; and
- Improving government and industry cooperation.

<u>Botnets – Today and into the Future</u>

A "bot" is a type of malware that allows an attacker to take control of an infected computer. Also known as "Web robots," bots are usually part of a network of infected machines, collectively known as a "botnet." These typically are made up of victim machines that stretch across the globe and are controlled by "bot herders" or "bot masters."[1] One recent study found that over 60% of traffic on the internet today is from bots.[2] About half of these bots are what we would call helpful bots, such as the automated web crawlers

[1] http://us.norton.com/botnet/

[2] http://incapsula.com/blog/bot-traffic-report-2013.html

that check to see that websites are running in good order or that index and update information for search engines. The others are malicious bots, the subject of today's hearing.

Botnet Uses

The uses for malicious bots are only limited by the imagination of the criminal bot master. The most common use for botnets is still for Distributed Denial-of-Service (DDoS) attacks. DDoS attacks occur when multiple infected systems are used to overload a website and render it unable to respond to legitimate requests. Another recent use of DDoS attacks has been to provide cover for another, more sophisticated attack. Organized crime groups have been known to launch DDoS attacks against banks to divert the attention and resources of the bank's security team while the main attack is launched, which can include draining customer accounts or stealing debit or credit card information.

Another common use for botnets is creating bitcoins, commonly known as bitcoin "mining." The mining process involves compiling information from recent bitcoin transactions and performing complex mathematical computations. Any single computer would take far too long to do the calculations to provide any value, so bot masters co-opt the processing power of thousands of hijacked computers to do so, thus "mining" valuable bitcoins for the bot master. The cost to unsuspecting victims is lost productivity.

Cybercriminals also use botnets as launch points for attacks or to amplify their own processing power and bandwidth for various criminal activities such as spam generation, malware distribution, click fraud,[3] and data storage. Bot masters also can rent out their botnets for illegal purposes and can generate hundreds of thousands of dollars by making their botnets available to other users.

Harvesting information such as passwords, credit card data, intellectual property, or other confidential information from infected computers is another common use for botnets. When this information is stored on a computer that is part of a botnet, the bot master has access to all of it – in an operational sense, they "own" that device. This information is often then sold to other criminals for fraudulent use.

Types of Botnets

The first botnets were centrally controlled – once a computer was infected, it would "call home" to a command and control (C&C) server to let the bot master know that the malware had been installed. Often, a bot master would then install additional software or otherwise solidify control over the infected device to ensure continued control over it. Much, if not all, of this activity is automated. At that point, the bot waited for further commands from its master – which could include any of the activities described above.

This centralized C&C model worked well, but had drawbacks. Though C&C servers can be hidden (and often are compromised computers themselves), they are potentially a single point of failure for a botnet. If the bot master loses control of a C&C server (or even just communications to or from the server) the whole botnet can be taken down. As a result, a growing number of botnets rely on a peer-to-peer (P2P) model, where any node in the network can act as both a client and a server. In a P2P botnet, each individual bot can distribute commands to other infected computers and as a result the network as a whole is highly resilient and resistant to takedowns.

Until now, virtually all botnets have been networks of infected laptop and desktop computers. However, in the past few years we have seen the first botnets comprised of mobile devices such as smart phones or tablets. And while the early reports of "smart" refrigerators sending spam proved to be incorrect,[4] we are seeing a major increase in compromised connected devices. As such, we fully expect that the coming "Internet of Things" will bring with it a future of "thingbots" of compromised connected devices that will range from appliances to home routers to digital video recorders – and who knows what else.

Efforts to Disrupt Botnets

Investigating and prosecuting cybercrime poses no less a challenge than does defending against cyber attacks. It is technically complex, and requires a level of expertise and training that many police agencies and prosecutors are just now beginning to develop. It is also resource intensive – the time and money required to see a case from inception through to a successful conviction is often substantial. The criminals know this, and indeed often count on it.

Despite these obstacles, law enforcement and the private sector – working together – have made significant progress in recent years. Not too long ago, numerous technological, cultural and organizational barriers prevented federal agencies from coordinating with each other or with industry on the investigation and prosecution of international cyber criminals. Those barriers have largely come down, and today we see that kind of cross-agency and public-private coordination on a regular basis.

Symantec's operation to bring down the *ZeroAccess* botnet, one of the largest botnets in history estimated at 1.9 million infected devices, is a good example of how effective coordination between industry and law enforcement can yield results. A key feature of the *ZeroAccess* botnet was its use of P2P architecture, which gave the botnet a high degree of availability and redundancy. Since there is no central C&C server, one cannot simply disable a few servers to bring down the botnet. *ZeroAccess* was primarily designed to deliver payloads to infected computers. These payloads performed two basic functions: click fraud and Bitcoin mining, with an estimated economic impact of tens of millions of dollars lost per year. In addition, we estimated that the cost of electricity alone to operate the botnet was as much as $560,000 per day.

Early in 2013, Symantec's engineers identified a weakness that offered a difficult, but not impossible, way to disrupt the botnet. One year ago today, Symantec began to sinkhole *ZeroAccess* infections, which quickly resulted in the detachment of over half a million bots. This meant that these bots could no longer receive any commands from the bot master and were effectively unavailable to the botnet both for spreading commands and for updating or installing new revenue generation schemes.[5] Later that year Microsoft filed a civil suit in the U.S. District Court for the Western District of Texas against the *ZeroAccess* botnet. These actions appear to have put an end to the botnet and the bot masters have halted their activity. They even included the words "White Flag" in the code of one of the last updates sent to infected computers.

Another significant win came last month, when the Federal Bureau of Investigation (FBI), the U.K. National Crime Agency, and a number of international law enforcement agencies mounted a major operation against the financial fraud botnet *Gameover Zeus* and the ransomware network *Cryptolocker*. *Gameover Zeus* was the largest financial fraud botnet in operation last year and is often described as one of the most technically sophisticated variants of the ubiquitous *Zeus* malware. Symantec provided technical insights into the operation and impact of both *Gameover Zeus* and *Cryptolocker*, and worked with a broad industry coalition

[4] "Despite the News, Your Refrigerator is Not Yet Sending Spam," http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam
[5] "Grappling with the ZeroAccess Botnet," http://www.symantec.com/connect/blogs/grappling-zeroaccess-botnet

and the FBI during this case. As a result, authorities were able to seize a large portion of the infrastructure used by the cybercriminals behind both threats.

In our view, the approach used in the *Gameover Zeus* operation was the most successful to date and should serve as a model for the future. A group of more than 30 international organizations from law enforcement, the security industry, academia, researchers, and ISPs all cooperated to identify the criminal element and technical infrastructure, develop tools, and craft messaging for users in order to collectively and aggressively disrupt this botnet. And while cyber criminals are resilient – recent reports are that a new gang is reconstituting parts of the defeated botnet – this successful model of public and private cooperation used to disrupt *Gameover Zeus* is one that can and should be repeated in the future.

A final example is the operation that helped to bring down the *Bamital* botnet, a major takedown that happened earlier this year. This effort was the culmination of a multi-year investigation conducted by a public-private partnership including Symantec, Microsoft, and law enforcement. The *Bamital* botnet had taken over millions of computers for criminal activities such as identity theft and click fraud, and threatened the $12.7 billion online advertising industry. This successful takedown is another example of what can be done when private industry and law enforcement join forces to go after cybercriminal networks.

Unfortunately, these examples highlight just how much still needs to be done. For while *ZeroAccess, Gameover Zeus*, and *Bamital* were successes for law enforcement and industry there are undoubtedly more - and likely larger – criminal rings operating today. The small number of successful cases such as these is not because governments do not want to pursue them, or because the criminals are not out there. The investigators and prosecutors are willing, and the private sector is eager to help. There are simply not enough resources – investigators, prosecutors, and judges – who can handle them. Put simply, as criminals migrate online, the FBI, the Secret Service, and state and local law enforcement agencies need more skilled personnel dedicated to fighting cybercrime.

<u>Assisting Victims of Botnets and Combating Cybercrime</u>

Preventing data theft caused by bots and protecting privacy starts with basic electronic device hygiene such as having security software installed, good patch management practices, using strong passwords, and recognizing suspicious emails. But that is just the start, because as we have seen in these high profile botnet cases, sophisticated and well-funded attackers are persistent and highly skilled. Of course, anti-virus software (AV) should be part of any security program and will stop known malicious software (malware), but it is just one element.

Today, even moderately sophisticated pieces of malware have unique signatures and can slip past systems that are using only AV software. Thus, strong security is layered security – in addition to basic computer hygiene and AV, consumers and organizations need comprehensive protection that includes intrusion protection, reputation-based security, behavioral-based blocking, and data loss prevention tools. These advanced tools look not just for known threats, but they can check the reputation of any file that is loaded on a computer and look for other behavior that could indicate the presence of previously unknown malware.

However, even with modern security suites, there is a risk that your device or network may become compromised. If that occurs, there are a number of things Symantec is doing to assist victims of botnets and other types of cybercrime. It is important to call out that these are not victimless crimes; at best, owners of infected computers suffer decreased functionality, and at worst they have their identities compromised and their bank accounts raided. Part of our efforts to stop botnets, and indeed cybercrime *writ large*, is helping individual victims.

In April 2014, we partnered with the National White Collar Crime Center (NWC3) on a new online assistance program to help victims file cybercrime complaints and to better understand the overall investigation process. I would like to thank Senator Whitehouse for your participation in the launch and support of the VictimVoice (victimvoice.org) initiative. Symantec also makes software available to the public as a whole (beyond our Norton Security customers) to assist them if they are infected by a botnet. For example, we offer free cleaning tools that allow victims of botnets and ransomware to remove malware from their system.[6]

Symantec is also active in organizations working to raise awareness and provide resources to fight botnets, including the Online Trust Alliance (OTA). The OTA works with the public and private sectors to address the threats resulting from botnets, and has created a multi-stakeholder botnet taskforce to take a holistic look at the botnet problem, including prevention, detection and remediation. Last year, through OTA, we contributed to the development of comprehensive guidelines for botnet remediation.[7] These guidelines have been used widely and reflect the best practices from a broad array of industry stakeholders. The OTA's other efforts include working with law enforcement, ISPs and web hosting companies in takedown efforts, promoting best practices to reduce the distribution of bots, and aiding users to reduce their vulnerabilities.

Another effort is the Industry Botnet Group (IBG) which was formed in January 2012 and was comprised of a group of companies, trade associations, and non-profit organizations concerned about the adverse impact of botnets. Established in response to a U.S. Department of Commerce request for information on ways to combat botnets, the group developed a set of principles to thwart botnets and encouraged voluntary efforts by government, industry, and users to raise awareness and reduce the effectiveness of botnets.

To combat cybercrime more broadly, Symantec participates in a number of public-private partnerships in the U.S. and abroad. As demonstrated in the botnet cases described above, we voluntarily share high-level cybercrime and cyber threat information through a number of different fora to help protect our customers and their networks. Of course, all of this is done in keeping with both our own strict privacy policies to protect our customer data, and all applicable privacy laws.

Some of our key partners in these areas are the National Cyber-Forensics and Training Alliance (NCFTA), InfraGard, and INTERPOL. The NCFTA is a good example of how private industry and law enforcement partnerships can yield real world success. The NCTFA is a Pittsburgh-based organization that includes more than 80 industry partners – from financial services to telecommunications to manufacturing – working with federal and international law enforcement partners to provide real-time cyber threat intelligence to an actionable level in order to identify threats and actors.

InfraGard, of which Symantec serves on the National Board of Advisors, is another example of how law enforcement can partner with both private industry and individuals to share information on cyber threats. This successful partnership between the FBI and members of the private sector is focused on intrusions and vulnerabilities affecting national critical infrastructure. Comprised of a coalition of more than 55,000 private and public sector members, InfraGard promotes ongoing dialogue and timely communication between its members and the FBI.

Because cyberspace is a domain without borders, where crimes are often committed at a great distance, every device in the U.S. is a potential border entry point, making investigation and prosecution of cybercrimes a difficult task. This reality makes international engagement on cybersecurity essential. For

[6] See http://www.symantec.com/security_response/removaltools.jsp

[7] "Anti-Botnet Remediation Best Practices, https://otalliance.org/resources/malicious-threats

example, Symantec recently partnered with AMERIPOL and the Organization of American States to publish a report that provides the most comprehensive snapshot to date of cybersecurity threats in the Latin American and Caribbean region. The goal was to raise awareness of cybercrime issues and promote the importance of cybersecurity throughout the region as a national and economic security imperative.

Symantec also maintains relationships around the world with international cyber response organizations and law enforcement entities including INTERPOL, EUROPOL, and dozens of national Computer Emergency Response Teams (CERTs) and police forces, by sharing the latest technological trends, the evolution of the threat landscape, and the techniques that cyber criminals use to launch attacks. Just last week, Symantec notified and provided detailed Indicators of Compromise (IoC) to more than 40 national CERTs around the world about a new threat we named *DragonFly*.[8] An ongoing cyber espionage campaign against a range of targets, mainly in the energy sector, gave attackers the ability to mount sabotage operations against their victims, which could have caused damage or disruption to energy supplies in affected countries. Among the targets of *Dragonfly* were energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers – the majority of the victims were located in the U.S., Spain, France, Italy, Germany, Turkey, and Poland. Quick and detailed notification was critical in mitigating the threat.

Unfortunately, both here in the U.S. and around the world, there is a critical shortage of investigators, prosecutors, and judges who are adequately trained to handle complex cybercrime cases. Recognizing this need, Symantec has a number of initiatives whereby we work with law enforcement organizations and non-profit safety groups to provide training and technical expertise, and to help facilitate global cooperation. For example, through our partnership with the National Center for Justice and the Rule of Law (NCRLJ) and the U.S. National Association of Attorneys General, Symantec has aided in training prosecutors in trying cybercrime cases as well as judges who adjudicate those cases.

This training can – and should – start when young lawyers are still in school. In March 2014, we sponsored the third annual cyber moot court competition at UCLA School of Law. The competition helps students develop their legal skills and introduces them to many of the difficult legal concepts surrounding cybercrime. Thirteen law schools sent teams to compete this year, and we hope to expand this program to reach other law schools.

Symantec also partners with international advocacy organizations, including the Canada-based Society for the Policing of Cyberspace (POLCYB), to provide training workshops to law enforcement officials and policymakers around the globe. To date, we have partnered with POLCYB and other organizations to train law enforcement officials and policy makers in more than 35 countries around the world. Last month, Symantec participated in a U.S. Department of State cybercrime workshop in Gabarone, Botswana, aimed at policy makers from the Southern Africa Development Community and other African regional organizations to raise awareness of the threats and impacts of cybercrime, including botnets.

<u>A Path Forward – Public and Private Cooperation</u>

Because cybercrime and botnets are a borderless problem, any effort to thwart them requires cooperation and coordination – between the government and the private sector, between governments, and within the private sector itself. In the private sector, we need to know that we can work with our government partners and with our private sector counterparts to disrupt botnets without having to look over our shoulder to

[8] "Dragonfly: Western Energy Companies Under Sabotage," http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat

ensure we are not running afoul of the law. To be clear, I am not talking about a blank check – what I am saying is that consistent with privacy protections and legal parameters, we need to be able to share cyber threat information and coordinate with our peers in industry and our partners in law enforcement quickly and efficiently.

Information sharing legislation that facilitates this cooperation, *while still protecting privacy*, is needed. Too often, security and privacy are portrayed as being in opposition, but in the digital world this is a false conflict because if our data is not secure, then neither is our privacy. At Symantec we have long supported civilian-led information sharing legislative proposals – and have also worked to ensure that they include requirements that an organization minimize personally identifiable information before information is shared. Improved information sharing – and corresponding legislation – is not a panacea, but it will give us another tool to help us work together by removing a barrier that may be keeping some organizations on the sidelines of the cybercrime fight.

Resources are also an issue in going after botnets and fighting cybercrime. As stated above, there are simply not enough investigators, prosecutors, and judges with the technical knowledge and experience to keep up with the growth of these types of cases. We recognize that the FBI, Secret Service, Department of Justice, and DHS have devoted significant new resources to cybercrime and cybersecurity in recent years, but the criminals are doing the same. If we want to improve cybercrime deterrence, the government needs to invest in new resources, as well as continue to grow successful partnerships with industry.

Lastly, the law governing cybercrime needs to be modernized. In the U.S., we need to look at amending laws such as the Electronic Communications Privacy Act, which was written before most Americans had heard of email or the Internet and when mobile phones were the size of bricks. This is no less true overseas, where most nations' laws also are playing catch up with the pace of innovation and technology. Another challenge today is that in order for governments to share cyber information internationally, we must still proceed through Mutual Legal Assistance Treaties (MLATs) and Letters Rogatory – processes first developed in the 1800s – and take far too long to address the real-time nature of cybercrime. To keep pace with 21st Century threats, the MLAT process should be overhauled and streamlined.

Conclusion

As this subcommittee knows better than most, we still face significant challenges in our efforts to take down botnets and dismantle cybercrime networks. But while there is still much work to be done, we have made progress. Today, at all levels, both government and industry recognize the imperative for cooperation to fight cybercrime. No single company or government can "go it alone" in the current threat landscape. The threats are too complex and the stakes are too high. Ultimately, defeating the threat of malicious botnets and the criminal networks behind them requires strong technical capabilities, effective countermeasures, industry collaboration and law enforcement cooperation to be successful.

At Symantec, we are committed to improving online security across the globe, and will continue to work collaboratively with international industry and government partners on ways to do so. Finally, I would also like to commend this subcommittee for its leadership on this important issue. Thank you again for the opportunity to testify, and I will be happy to answer any questions you may have.

Testimony of

Paul Vixie, Chairman & CEO
Farsight Security, Inc.

before the
Subcommittee on Crime and Terrorism
United States Senate Committee on the Judiciary

Hearing on
Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle
Cybercriminal Networks

July 15, 2014

I. INTRODUCTION

Good afternoon Mr. Chairman, Ranking Member Graham, and Members of the Subcommittee. Thank you for inviting me to testify on the subject of botnet takedowns.

My name is Paul Vixie, and I am the Chairman and Chief Executive Officer of Farsight Security, a commercial Internet security company. I am speaking today in my personal capacity based on a long history of building and securing Internet infrastructure. I am also here at the behest of the Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG), a non-profit Internet security association whose international membership is actively working to improve Internet security conditions worldwide.

I have first-hand knowledge of these matters from my experience in the Internet industry since 1988. My background includes serving as the Chief Technology Officer for Abovenet/MFN, an Internet Service Provider (ISP); serving as the founder and CEO of MAPS, the first anti-spam company; and acting as the operator of the "F" DNS root name server. I have also been involved in Internet standards work in the Internet Engineering Task Force (IETF) and policy development work in the Internet Corporation for Assigned Names and Numbers (ICANN). In addition, I served for nine years on the board of trustees of ARIN, a company responsible for allocating Internet address resources in the United States, Canada, and parts of the Caribbean. I presently serve on the ICANN Security and Stability Committee (SSAC) and the ICANN Root Server System Advisory Committee (RSSAC). I am the author of several Internet standards related to the Internet Domain Name System (DNS) and was for eleven years the maintainer of BIND, a popular open source DNS software system. It was for my work on DNS and BIND that I was inducted earlier this year into the Internet Hall of Fame. My remarks today reflect my ongoing goal of fostering improvements in botnet takedown activities by the non-profit, for-profit, and law enforcement sectors.

II. LESSONS FROM CONFICKER AND GHOST CLICK

I would like to start by reviewing several successful botnet takedown efforts in recent years, since commonalities among these successes may prove instructive.

In 2008 the Conficker worm was discovered and by mid-2009 there were over ten million infected computers participating in this botnet. I had a hands-on-keyboard role in operating the data collection and measurement infrastructure for the takedown team[1], in which competing commercial security companies and Internet Service Providers – most being members of M^3AAWG – cooperated with each other and with the academic research and law enforcement communities to mitigate this global threat.[2]

In 2011 the US Department of Justice led "Operation Ghost Click" in which a criminal gang headquartered in Estonia was arrested and charged with wire fraud, computer intrusion, and conspiracy. The "DNS Changer" botnet included at least 600,000 infected computers and the mitigation task was complicated by the need to keep all of these victims online while shutting off the criminal infrastructure the victims at this point depended on[3]. My employer, Internet Systems Consortium (ISC), was the court appointed receiver for the criminal's Internet connectivity and resources, and I personally prepared, installed, and operated the replacement DNS servers necessary for this takedown.

Each of these examples shows an ad-hoc public/private partnership in which trust was established and sensitive information including strategic planning was shared without any contractual framework. These takedowns were so-called "handshake deals" where personal credibility, not corporate or government heft, was the glue that held it together and made it work. And in each case the trust relationships we had formed as members of M^3AAWG were key enablers for rapid and coherent reaction.

Each of these takedowns is also an example of modern multilateralism in which intent, competence, and merit were the guiding lights. The importance of multilateralism cannot be overemphasized: We have found that when a single company or a single agency or nation "goes it alone" in a takedown action, the result has usually been catastrophe. The Internet is hugely interdependent and many rules governing its operation are unwritten. No amount of investment or planning can guarantee good results from a unilateral takedown action. Rather, takedown actors must work in concert and cooperation with a like-minded team representing many crafts and perspectives, in order to maximize benefit and minimize cost – and I refer specifically to the collateral costs borne by uninvolved bystanders.

For example, Conficker's second major version generated 50,000 (fifty thousand) domain names per day that had to be laboriously blocked or registered in order to keep the control of this botnet out of the hands of its criminal authors. Complicating the situation, these 50,000 domain names were split up across 110 different "country code" top-level domains that are each the property of a sovereign nation. The registries for these domains are a mix of private and public institutions, some with national government oversight and many without. Almost all of the 110 registries agreed to cooperate, which involved sharing technical plans and data, as well as strategic plans and calendars.

Similarly, Operation Ghost Click required cooperation between United States and Estonian national law enforcement agencies, as well as competing national and multi-national ISPs and Internet security companies, and an eclectic collection of Internet researchers and adventurers. This diverse team worked together for a single common cause which was to protect the Internet's end users and restore the Internet's infrastructure after an extraordinary breach.

Privacy deserves a special mention. In any takedown of criminal infrastructure, it is vital that end user privacy be protected according to the greatest common denominator of the laws or rules governing each participant in the coordinated takedown effort. So it was in Conficker, where victim event data that showed time stamps and unique IP addresses were only made available on a trusted, need-to-know basis. This information was only shared either with responsible scientists for studies conforming to international ethical guidelines for human subjects research, or with ISPs and anti-virus companies for the narrow and specific purpose of identifying and notifying victims with the end goals of cleanup and remediation.

Privacy protections during Operation Ghost Click were even more rigorous. The court-appointed receiver who operated the replacement DNS servers deliberately gathered the minimum possible data about each victim, which included the IP address, time stamp, and port number – but no end-user DNS lookup names. Furthermore, the FBI and DOJ team members declared themselves unwilling to hold or even receive victim specific data, so the court-appointed receiver delivered the victim records directly to the researcher and clean-up teams, subject to non-disclosure terms.

The ad-hoc nature of these public/private partnerships may seem like cause for concern, but I hope you will consider the following: First, this is how the Internet was built and how the Internet works; second, this is how criminals work with other criminals. We would not get far by trying to solve these fast-evolving global problems with top-down control or through government directives and rules. Bot masters are constantly innovating, both by devising new ways to penetrate networks and new methods of avoiding detection. Effective response to, and remediation of, botnet attacks requires a coordinated effort that is flexible, nimble, and capable of quickly identifying and adapting to a dynamic and changing threat landscape. While government has a role to play in the takedown of criminal infrastructure such as botnets, it can be most effective by continuing to support the participation in ad-hoc public/private partnerships by agencies such as Justice (for example, see the FBI's involvement in the National Cyber-Forensics and Training Alliance [NCFTA]) and Homeland Security (for example, see the United States Computer Emergency Readiness Team [US-CERT] and the SEI/CMU CERT).

As another takeaway, I note that these two successful takedown exercises were both zero-fee events – no one was asked to "pay to play." The shared goal of protecting Internet end users and restoring the Internet's infrastructure requires a perfectly level playing field, and the only money which changed hands in Operation Ghost Click was a modest contract for technical services between the DOJ and the court-appointed receiver.

III. EFFECTIVE ACTION REQUIRES UNDERSTANDING HOW BOTNETS ORIGINATE AND PROLIFERATE

I'd like to take a moment to explain where botnets come from and what makes them so attractive to criminals and also what makes them possible.

A botnet is literally a "network of robots," where by "robot" we mean a computer that has been captured and made to run software neither provided by the computer's maker nor authorized or installed by its owner. The Internet now reaches billions of end users, as well as tens of millions of unattended "servers" including alarming growing number of industrial control systems. Every Internet-connected device has some very complex software including an operating system, installed applications, and ephemeral "plugins." The only hard and fast requirement for any of this software is "interoperability," meaning, it merely has to work.

From its humble academic origins in 1969 to the present planetary-scale digital fabric interconnecting most humans and facilitating almost all commerce, the Internet has seen continuous wildcat growth. As a platform for innovation, the Internet is unequaled in all of human history for the value it has created and the tools it has made available to every person in every nation. The level of freedom allowed to innovators on the Internet is unprecedented – pretty much any smart person or team can try out almost any idea, with a built-in global audience and perhaps an immediate global market as well.

The invisible cost of this growth and innovative value creation is that much of the software we run on many of our connected devices was given wide exposure and perhaps forgotten by its maker without receiving "red team" testing to check for vulnerabilities. The challenge for the Internet is that today there is perhaps more assurance that a U.L. Listed toaster oven will not burn our house down than there is that some of our vastly more expensive and powerful Internet-connected devices are insulated from becoming a tool of online criminals.

The economics of this situation also can be challenging, since in the fast-changing, high-growth Internet-enabled economy the winners are characterized by short time to market, low cost, and high volume. Innovators may not always have the time or resources to address potential security issues, so we live in a culture of "patching it later." During the preparation of these remarks, I read news reports of an Internet-enabled light bulb, part of the "Internet of things," that was found to be vulnerable to a simple attack in which it would expose the local wireless network password to anyone who asked. It is extremely unlikely that any of these flawed light bulbs can be patched or that their owners can or will be informed of the need to return the product for a refund or exchange. So while the world needs the Internet and the Internet's powers of economic growth and innovation, the cost to the world is that many tens of millions of connected devices can easily and quite often do become tools for criminals. Some companies know this and are addressing it, but much work remains.

But the pace of innovation and adaptation on the Internet is being matched by the pace of innovation and adaptation by criminal bot masters. After a software flaw leading to vulnerability is found and circulated, it is quickly exploited for criminal purposes. The first step is to use the flaw to install software used by criminals to manage the new computer as part of a botnet. Later steps will be to install specific software tools to facilitate various kinds of online crime like DDoS attacks, spamming, key logging, credential theft, or identity theft. The most important role of every member of a botnet is: *find and infect more victims.* Thus virtually all software flaws are exercised indirectly, using other infected computers. Criminals can operate their infrastructure through so many layers of proxies and middle-men that it's almost impossible to trace most criminal acts back to their actors. As corollaries, it's safe to say two things: (1) Most Internet crime could not exist without botnets; and (2) Botnets could not exist absent a never-ending series of software flaws in Internet connected devices.

This is not a call for regulatory relief. The Internet's success has come organically; that is, not just without a plan but precisely because there was no plan. No national government or super-national governance body could, or should try to, put this genie into a bottle. Rather, we must take stock of some long-invisible costs and make informed decisions as a nation and as a society on which of the Internet's costs we should just live with versus which costs are high enough that we should seek out cheaper alternatives. The primary ways to lower these costs are no different than any non-Internet field: (1) Understand our situation; (2) Make our choices with eyes wide open; and (3) Invest or front-load wherever it will reduce costs in the long run.

Finally, I'd like to quote an ICANN Security and Stability Advisory Committee (SSAC) report from 2002:

> With the advent of high speed "always on" connections, these PCs add up to either an enormous global threat, or a bonanza of freely retargetable resources, depending upon one's point of view.[4]

Regrettably, the major trend in the twelve years since that report was written is growth – more Internet connected devices, more software flaws, more botnets, and more crime.

IV. STEPS FOR THE FUTURE

Next, I'd like to describe what I think are some practical and effective next steps we can take toward some short and medium term goals. As you'll see, I believe that we can get the most traction by going after the causes, enablers, and attractions of botnets, rather than just beefing up our ability to take down botnets.

Awareness campaigns have played a notable role in slowing the spread of human diseases such as tuberculosis and HIV. Given the danger that an unpatched and undefended Internet connected device can pose to the world's economy as well as to the privacy and safety of its owner and other humans, why would we do less to stop the spread of botnets? I hope to see the day when every user of the Internet knows that if their device is out of date and terribly slow, it is probably infected with malicious software that makes the device steal their identity, send spam, and participate in DDoS attacks.

The US Government is one of the world's largest buyers of Information Technology (IT). Any technical requirement that becomes part of the Federal Information Processing Standards (FIPS) stands a good chance of becoming a de-facto standard for the world. Since DDoS attacks often rely on the lack of Source Address Validation (SAV) by an ISP, perhaps we should investigate requiring SAV by date-certain for all ISPs and hosting or cloud service providers who wish to sell services to the US Government.

Ensuring the security of critical infrastructure is a high priority for both government and industry. It may be useful to explore empancling a blue ribbon committee to identify and recommend best practices for securing network and server architecture operating industrial control systems, especially as it rclates to connected devices, connections between the hot side and the outside, and softwarc testing and patching protocols for those systems. Some of the Conficker-infected computers we tracked in 2008 and 2009 turned out to be industrial controllers for medical equipment including in some cases human life/safety monitors used in surgical operating theatres. While there may be some subtleties involved in getting these embedded computers patched without triggering full recertification, there's no question that these computers should not be connected to the open Internet, or that the staff's first clue that they have a problem should not be a phone call from the Conficker Working Group. We are now a connected society, and we need to find more ways to front-load security protections into Internet-connected services and offerings. To this end, government should continue to support and encourage industry-led groups like M^{3}AAWG – which has been active in publishing reports and developing voluntary practices aimed at strengthening and facilitating botnet detection and remediation – and public/private partnerships like NCFTA.

V. CONCLUSION

I've given a very brief overview of the botnet problem, its causes, its impact, and its likely future assuming we allow nature to take its course. I'd like to leave you with the following thoughts:

1. The Internet is the greatest invention in recorded history, in terms of its positive impact on human health, education, freedom, and on every national economy.
2. We have necessarily cut some corners on device and software safety and quality in order to innovate at breakneck speed from 1969 to now – time-to-market, not resistance to takeover, has often been our overriding engineering principle.
3. The Internet is also therefore the greatest invention in recorded history in terms of its negative impact on human privacy and freedom, as evidenced by the massive and continuing illicit transfer of wealth from productive people and countries toward unproductive people and countries.
4. Our democratic commitment to the rule of law has very little traction on the Internet compared to how the rule of law works in the real world. The Internet is borderless and lawless, but carries more of the world's commerce every year.
5. These problems manifest as "botnets" which are networks of robots, where the robots in question are using our connected devices in ways we never agreed to.
6. Takedown of criminal infrastructure including "botnets" must be approached not just as reactions after the fact but also as prevention by attacking the underlying

causes.

7. Takedown is no single agency's or any single company's job, and unilateralism never ends well in any case – so, cooperation and multilateralism must be our guiding lights.
8. The US Department of Justice is the envy of the world in its approach to takedown and its awareness of the technical and social subtleties involved, with a special shout-out to NCFTA, a public/private partnership with strong FBI ties.
9. No legislative or regulatory relief is sought in these remarks – the manner in which government and industry have coordinated and cooperated on botnet takedown efforts have underscored the effectiveness of public/private partnerships that afford all affected parties the necessary degree of flexibility and adaptability to face and eliminate botnet threats.

Mr. Chairman, Ranking Member Graham and Members of the subcommittee, this concludes my written statement. Thank you again for this opportunity to speak before you today on this important topic, and I would be happy to answer your questions.

[1] *Conficker Working Group*, http://confickerworkinggroup.org/wiki/
[2] *Worm: The First Digital World War*, Mark Bowden, 2011, ASIN B005IGBHU8
[3] *DNS Changer Working Group*, http://www.dcwg.org/
[4] *Securing the Edge*, Paul Vixie, 2002, https://archive.icann.org/en/committees/security/sac004.txt

OTA
Online Trust Alliance

Written Testimony

Craig D. Spiezle, Executive Director & Founder
Online Trust Alliance

Before the
Senate Judiciary Committee's
Subcommittee on Crime & Terrorism

Taking Down Botnets: Public and Private Efforts to
Disrupt and Dismantle Cybercriminal Networks

July 15, 2014

Chairman Whitehouse, Ranking Member Graham and members of the Committee, thank you for the opportunity to testify before you today. I also would like to thank you for your leadership in focusing attention to this important topic which is impacting users and businesses throughout the country.

My name is Craig Spiezle. I am the Executive Director and President of the Online Trust Alliance. OTA is a 501c3 non-profit, with the mission to enhance online trust and empower users, while promoting innovation and the vitality of the internet.

My background includes over a decade focusing on fighting online abuse, security and privacy threats. I have worked on a range of technologies and practices including developing and advancing anti-spam standards, anti-phishing technologies and introducing privacy controls providing users the ability to control the collection and use of their personal data.

OTA collaborates with several leading organizations fighting online abuse including the Anti-Phishing Working Group, (APWG), CA/Browser Forum, Center for Democracy and Technology (CDT), Email Service Provider Coalition, (ESPC), the Identity Theft Council, InfraGard, the International Association of Privacy Professionals (IAPP), the London Action Plan, Merchant Risk Council, StopBadware and others.

Botnets and associated cybersecurity exploits pose a significant risk to users, businesses and governments around the world. Increasingly bots are deploying key loggers and ransomware driving identity theft and bank account take-overs holding user's personal data, photo and health records hostage. Consumers innocently visiting trusted web sites are being compromised by malicious ads known as malvertising, while other bots are being used to cripple banking sites and make government services inaccessible.

It is important to recognize fighting bots is not just a domestic activity. Any effort requires a strategy to address international networks as cyber criminals intentionally operate beyond our borders. Criminals are leveraging the jurisdictional limitations of law enforcement and are proving to be nimble and innovative. They collaborate, share data and tools and often operative with impunity. Left unabated, they are a significant threat or our nation's critical infrastructure, to our economy and to users' privacy.

In my testimony I will discuss the following key areas:

1. Status of industry efforts
2. Need for a multifaceted anti-bot strategy
3. Role of takedown and law enforcement
4. Threat intelligence & data sharing
5. Privacy safeguards

Industry Efforts

Efforts to help combat botnets have been embraced by a range of public and private efforts. As an example, the FCC's Communications Security, Reliability and Interoperability Council (CSRIC), a FCC Federal advisory committee, last year developed a voluntary U.S. Anti-Bot Code of Conduct for ISPs, (ABC for ISPs). [1] [2] This code, modeled on efforts originally developed in Australia and Japan, has been publicly supported by ATT, Century Link, Comcast, Cox Communications and others. This code is an important example of the industry's ability to self-regulate.

In parallel, OTA has facilitated several multi-stakeholder efforts and working groups. These include publishing remediation and notification best practices and anti-bot guidelines for hosters and cloud service providers.[3] [4] [5] Adoption of these best practices by ISPs and other intermediaries will pay dividends helping protect users and aid in the remediation of their devices, data and privacy.

Multifaceted Strategy

Fighting botnets requires a holistic and global multi-stakeholder strategy. As outlined in Exhibit A, OTA advocates a five prong anti-bot framework including: Prevention, Detection, Notification, Remediation and Recovery. The Exhibit outlines a partial list of tactics and counter measures, which underscores the need for increased industry collaboration, research and two-way data sharing with the public and private sectors.

[1] http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iv

[2] http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf

[3] https://otalliance.org/system/files/files/resource/documents/ota_botnet_notification_whitepaper2012.pdf

[4] https://otalliance.org/system/files/files/best-practices/documents/ota_2013_botnet_remediation_best_practices.pdf

[5] Https://otalliance.org/resources/botnets

Law Enforcement & Takedown Efforts

Law enforcement efforts are an important component to fighting online threats serving three major functions; 1) disrupting command and control hosts used by cybercriminals to run their botnets, 2) gathering evidence and intelligence and 3) bringing criminals to justice.[6]

Law enforcement can't fight today's sophisticated cyber criminals alone. They need help from industry partners. Similarly, the private sector can't fight cyber criminals without help from law enforcement. A trusted partnership is required. Noteworthy examples of collaboration is the DNS Changer takedown, impacting four million computers located in over 100 countries and similar efforts led by Microsoft and Symantec.[7]

Botnet take-downs and related efforts need to be taken with care and respect to three major considerations: 1) the risk of collateral damage to innocent third parties, 2) errors in identifying targets for mitigation and 3) respecting users' privacy. For example, taking down an entire web hoster because they have a handful of bad customers may be an example of unacceptable collateral damage. At the same time hosters and ISPs cannot hide behind bad actors and must take reasonable steps to help prevent the harboring of criminals and enabling cybercrime activity.

It is important to note that other anti-abuse tactics run similar risks including the unintended sharing of personal and sensitive information. The ISP and the anti-spam community continually fight spam which unfortunately can result in the blocking of legitimate senders. Bot traffic has been misidentified by ISPs and security vendors have temporarily blocked and re-directed residential users' internet access. Web browsers run the risk of misidentifying phishing sites and AV solutions can mistakenly block downloads and web content. Recognizing these risks, the public and private sector must establish

[6] http://en.wikipedia.org/wiki/Botnet

[7] http://www.fbi.gov/newyork/press-releases/2011/manhattan-u.s.-attorney-charges-seven-individuals-for-engineering-sophisticated-internet-fraud-scheme-that-infected-millions-of-computers-worldwide-and-manipulated-internet-advertising-business

risk assessment procedures while staffing 24/7 remediation and escalation processes to remediate any unintended business and user impact.

Data Sharing

Data sharing between law enforcement and industry colleagues has the promise of being one of the most impactful tools in our arsenal. Data sharing must be reciprocal, with law enforcement providing data back to industry. Effective sharing requires exchanges that are dynamic and assure confidentiality. While today such sharing is occurring within individual sectors, expanded collaboration is needed between sectors such as retail, financial services and advertising networks. In the absence of this collaboration, cybercriminals move from one industry to another, sending malicious spam one day and perpetrating click-fraud and malvertising the next.[8]

Several industries have stood up Information Sharing and Analysis Centers (ISACs). These provide the ability to share data with each other, accelerating the deployment of best practices and threat detection capabilities.[9]

Privacy Controls & Considerations

The privacy landscape is rapidly evolving in the US, EU and other countries, ranging from the "right to be forgotten" and "Do Not Track", to restrictions on data sharing with third parties. Unfortunately threat intelligence data can often contain personally identifiable information, (PII). This underscores the importance that privacy be at the foundation of all fraud prevention and data sharing practices. Safeguards must be established including traffic monitoring by ISPs and data sharing among intermediaries including banks, websites and the AV community with law enforcement. Parties need to adhere to the FTC's Fair Information Practice Principles (FIPPS) and related sectorial regulations and adopt de-identification practices.[10]

[8] http://www.businessinsider.com/study-bots-will-waste-116b-in-ad-spend-in-2014-2014-1
[9] http://www.isaccouncil.org/
[10] http://en.wikipedia.org/wiki/FTC_Fair_Information_Practice

These privacy concerns can be easily addressed. When data is collected and used exclusively for threat detection, entities should be afforded "safe-harbor", providing that the data collected and shared is not used or retained for any other purpose. Conversely, industry needs assurances that law enforcement will not use such data for purposes other than fighting cybercrime.

Shared Responsibility

Every stakeholder has a responsibility to take action against these threats. We need to work together, be nimble and innovative. Progress has been with some ISPs and hosters, but a renewed focus and greater commitment from industry is required. As the Internet of Things, the smart grid and wearable technologies becomes prevalent, we need to look beyond the desktop. For example today mobile devices are increasingly being targeted by bots. This requires a renewed focus and investment from the mobile community including the role of app platforms and OS providers to increase the scrutiny and vetting of apps they host.

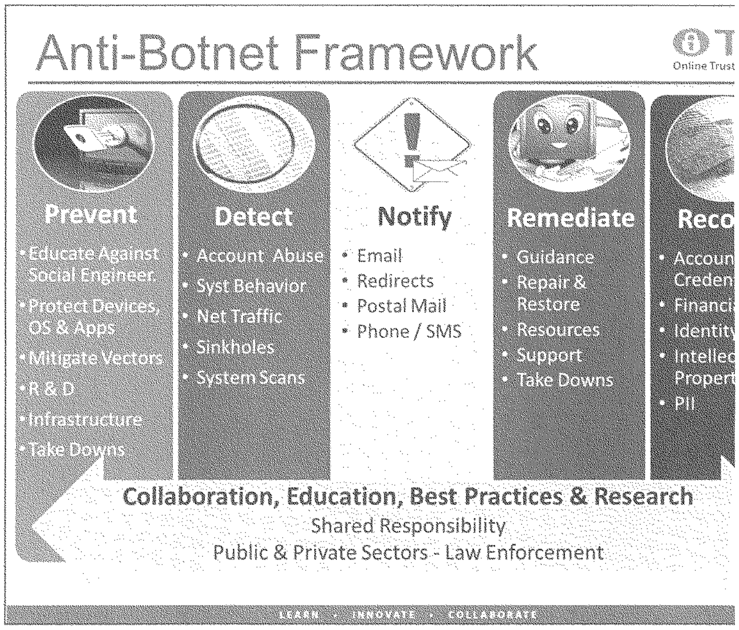
Summary

In summary, it is important to recognize there is no absolute defense against determined criminals. They will continue to exploit our systems and users, requiring all stakeholders and intermediaries to take action. We have a shared responsibility to increase investments in data sharing and adopt privacy enhancing practices, while finding new approaches to work with law enforcement and expand international cooperation.

Working together we can make the internet more trustworthy, secure and resilient while promoting innovation.

Thank you and I look forward to your questions.

Exhibit A – OTA Anti-Botnet Framework



Anti-Botnet Framework

Online Trust

Prevent
- Educate Against Social Engineer.
- Protect Devices, OS & Apps
- Mitigate Vectors
- R & D
- Infrastructure
- Take Downs

Detect
- Account Abuse
- Syst Behavior
- Net Traffic
- Sinkholes
- System Scans

Notify
- Email
- Redirects
- Postal Mail
- Phone / SMS

Remediate
- Guidance
- Repair & Restore
- Resources
- Support
- Take Downs

Reco
- Accoun Creden
- Financi
- Identity
- Intellec Propert
- PII

Collaboration, Education, Best Practices & Research

Shared Responsibility

Public & Private Sectors - Law Enforcement

LEARN • INNOVATE • COLLABORATE

NEWS FROM U.S. SENATOR SHELDON WHITEHOUSE

FOR IMMEDIATE RELEASE
July 15, 2014

Contact: Seth Larson
(202) 228-6291 (press office)

Opening Statement of Sheldon Whitehouse Chairman, Judiciary Subcommittee on Crime and Terrorism Hearing on: "Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks"

As Prepared for Delivery

Washington, DC – Welcome to today's hearing entitled "Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks."

Today, this Subcommittee will hear testimony about botnets and the threat they pose to our economy, our privacy, and our national security. A botnet is simply a network of computers connected over the internet that can be instructed to carry out specific tasks – typically without the owners of those computers knowing it.

Botnets have existed in various forms for well over a decade, but they are now recognized as the weapon of choice for cyber criminals. It is easy to see why: A botnet can increase the computing resources at a hacker's disposal exponentially, while helping conceal the hacker's identity. A cyber criminal with access to a large botnet can command a virtual army of millions – most of whom have no idea they have been conscripted.

Botnets enable criminals to steal individuals' personal and financial information, plunder bank accounts, and commit identify theft on a massive scale. For years, botnets have sent most of the spam we all receive; the largest botnets are capable of sending billions of spam messages per day. Botnets are used to launch distributed denial of service (or DDoS) attacks, which can shut down websites by overwhelming them with traffic – a constant danger for businesses in every sector of our economy. The only limit to the malicious purposes for which botnets can be used may be the imaginations of the criminals who control them – and when a hacker runs out of uses for a botnet, he can simply sell it to another criminal organization to use for an entirely new purpose.

Let's be clear: the threat from botnets is not just to our wallets. Botnets are effective weapons not merely for those who want to steal from us, but also for those who wish to do us far more serious harm. Experts have long feared the next 9/11 may be a cyber attack. If that is the case, it is likely that a botnet will be involved. Simply put, botnets threaten the integrity of our computer networks, our personal privacy, and our national security.

In recent years, the government and the private sector have launched aggressive enforcement actions to disrupt and disable individual botnets.

The techniques used to go after botnets are as varied as the botnets themselves. Many of these enforcement actions use the court system to obtain injunctions and restraining orders, utilizing innovative legal theories combining statutory claims under the Computer Fraud and Abuse Act and other laws with ancient common-law claims like trespass to chattels.

In 2011, the government obtained – for the first time – a court order that allowed it to seize control of a botnet using a substitute command and control server. As a result, the FBI launched a successful takedown of the Coreflood botnet, freeing 90% of the computers it had infected in the United States.

Microsoft, working with law enforcement, has obtained several civil restraining orders to disrupt and, in some cases, take down individual botnets, including the Citadel botnet, which was responsible for stealing hundreds of millions of dollars from bank accounts. And earlier this year, the Justice Department and the FBI, working with the private sector and law enforcement agencies around the world, obtained a restraining order allowing them to take over the Gameover Zeus botnet. This action was particularly challenging, because the botnet relied on a decentralized command structure that was designed to thwart efforts to stop it.

Each of our witnesses today has played a role in efforts to stop botnets. I look forward to learning more about these and other enforcement actions and the lessons that have been learned from them. We must recognize that enforcement actions are just one part of the answer, so I am interested in hearing about how we can better inform computer users of the dangers of botnets and what other steps we can take to address this threat.

My hope is that this hearing starts a conversation among those dealing day-to-day with the botnet threat and those of us in Congress who are deeply concerned about that threat. Congress, of course, cannot and should not dictate tactics for fighting botnets; that must be driven by the expertise of those on the front lines of the fight. But Congress does have an important role to make sure that there is a solid legal foundation for enforcement actions against botnets and clear standards governing when they can occur. We must also ensure that botnet takedowns and other actions are carried out in a way that protects consumers' privacy, while recognizing that botnets themselves represent one of the greatest privacy threats computer users face today. And we must make sure our laws respond to a threat that is constantly evolving, and encourage, rather than stifle, innovative efforts to disrupt cyber criminal networks.

I look forward to starting this conversation today and to continuing it in the months ahead. I thank my distinguished Ranking Member for being such a terrific colleague on these cyber issues. I thank you all for participating in this hearing and for your efforts to protect Americans from this dangerous threat.

###

Questions for the Record
"Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks"
July 15, 2014
Senator Sheldon Whitehouse

Richard Boscovich:

1. As we discussed, the Subcommittee is exploring possible legislation to address the botnet threat. What specific proposals would you recommend we include in such legislation?

2. Do you have any comments on the legislative proposals that Assistant Attorney General Caldwell discussed in her testimony?

3. How do we ensure that our laws give the public and private sectors the tools they need to respond to the botnet threat, while at the same time recognizing that the threat itself – and therefore the most effective responses to it – are constantly evolving?

Questions for the Record
"Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks"
July 15, 2014
Senator Sheldon Whitehouse

Cheri McGuire:

1. As we discussed, the Subcommittee is exploring possible legislation to address the botnet threat. What specific proposals would you recommend we include in such legislation?

2. Do you have any comments on the legislative proposals that Assistant Attorney General Caldwell discussed in her testimony?

3. How do we ensure that our laws give the public and private sectors the tools they need to respond to the botnet threat, while at the same time recognizing that the threat itself – and therefore the most effective responses to it – are constantly evolving?

Questions for the Record
"Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks"
July 15, 2014
Senator Sheldon Whitehouse

Craig Spiezle:

1. As we discussed, the Subcommittee is exploring possible legislation to address the botnet threat. What specific proposals would you recommend we include in such legislation?

2. Do you have any comments on the legislative proposals that Assistant Attorney General Caldwell discussed in her testimony?

3. How do we ensure that our laws give the public and private sectors the tools they need to respond to the botnet threat, while at the same time recognizing that the threat itself – and therefore the most effective responses to it – are constantly evolving?

Questions for the Record
"Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks"
July 15, 2014
Senator Sheldon Whitehouse

Dr. Paul Vixie:

1. As we discussed, the Subcommittee is exploring possible legislation to address the botnet threat. What specific proposals would you recommend we include in such legislation?

2. Do you have any comments on the legislative proposals that Assistant Attorney General Caldwell discussed in her testimony?

3. How do we ensure that our laws give the public and private sectors the tools they need to respond to the botnet threat, while at the same time recognizing that the threat itself – and therefore the most effective responses to it – are constantly evolving?

Questions for the Record
"Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks"
July 15, 2014
Senator Sheldon Whitehouse

Cheri McGuire:

1. As we discussed, the Subcommittee is exploring possible legislation to address the botnet threat. What specific proposals would you recommend we include in such legislation?

Streamlining and modernizing the Mutual Legal Assistance Treaties (MLATs) would have an immediate impact on law enforcement's ability to share information, investigate and prosecute cybercriminals. While the MLAT system today provides an internationally recognized and well understood legal framework, it was first developed in the 1800s – and takes far too long to address the real-time nature of cybercrime. To keep pace with 21st Century threats, the MLAT process should be overhauled, streamlined and properly funded. In addition, the Computer Fraud and Abuse Act (CFAA) should be amended to clarify that trafficking in access to botnets is a criminal offense. Today, a criminal can sell, or even rent, access to a botnet to steal personal or financial information or conduct DDOS attacks and not be in violation of the CFAA. The CFAA should be amended to include trafficking in access to botnets.

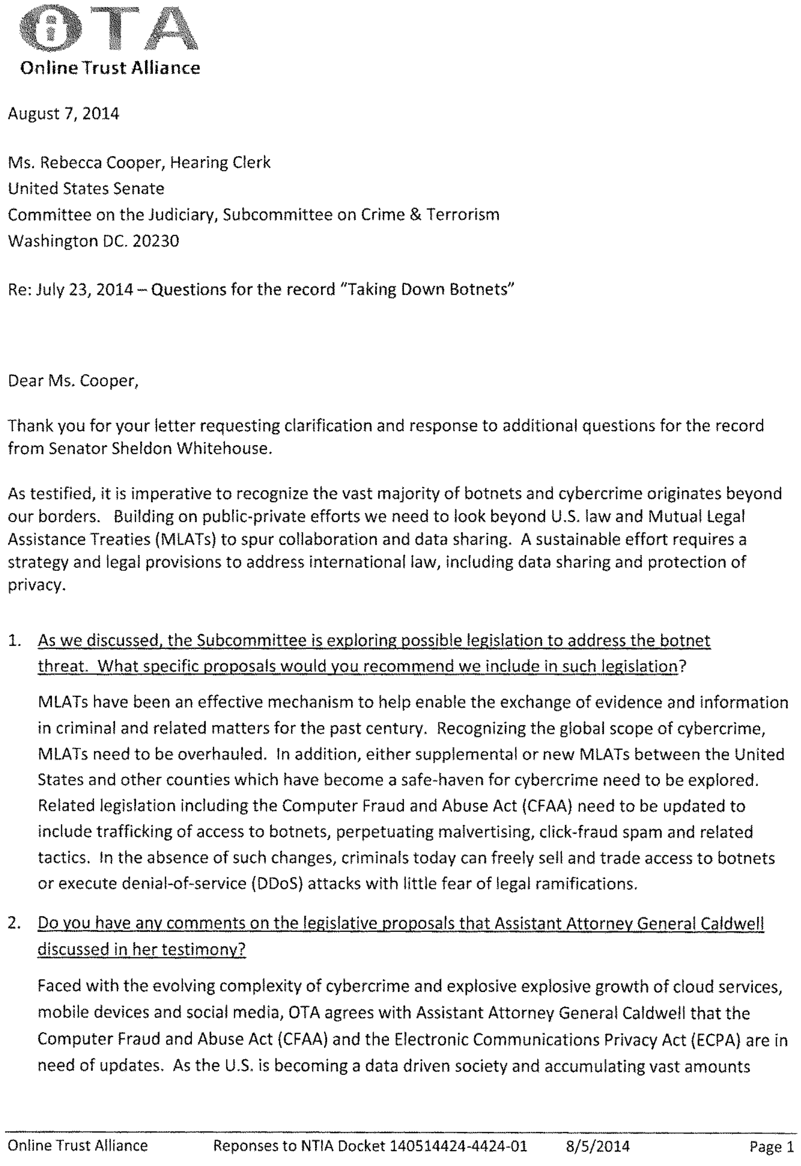
2. Do you have any comments on the legislative proposals that Assistant Attorney General Caldwell discussed in her testimony?

I agree with Assistant Attorney General Caldwell that many of the laws that now govern cybercrime need updating, and that the Computer Fraud and Abuse Act (CFAA) and the Electronic Communications Privacy Act (ECPA) need to be updated to reflect modern technology. Specifically, communications and storage technology such as email, cloud, and social networking, should be afforded the same legal protections as documents stored on a hard drive or letters filed in a drawer and secured in your home. The government should obtain a search warrant based on probable cause before it can compel a service provider to disclose a user's private communications or documents stored online. With that *said, any update must be done with care to ensure that the statutes are flexible enough that they can adapt as new technologies emerge.*

3. How do we ensure that our laws give the public and private sectors the tools they need to respond to the botnet threat, while at the same time recognizing that the threat itself – and therefore the most effective responses to it – are constantly evolving?

As I noted above, updating ECPA and the CFAA and modernizing the MLAT process will help to create a legal environment that will allow the public and private sectors to work cooperatively to respond to botnets. Information sharing legislation – crafted in a way that both facilitates sharing and that protects privacy – is also essential. Congress can also play an important role in raising public awareness about the continually evolving threat of botnets and cybercrime – as you have done with your hearings. Finally, it is important that Congress continue to engage with the private sector so that together we can all ensure that any new laws do not hamstring innovation and succeed in promoting privacy protections and supporting international cooperation and standards.

Responses of Craig D. Spiezle to Questions Submitted by Senator Whitehouse



OTA
Online Trust Alliance

August 7, 2014

Ms. Rebecca Cooper, Hearing Clerk
United States Senate
Committee on the Judiciary, Subcommittee on Crime & Terrorism
Washington DC. 20230

Re: July 23, 2014 – Questions for the record "Taking Down Botnets"

Dear Ms. Cooper,

Thank you for your letter requesting clarification and response to additional questions for the record from Senator Sheldon Whitehouse.

As testified, it is imperative to recognize the vast majority of botnets and cybercrime originates beyond our borders. Building on public-private efforts we need to look beyond U.S. law and Mutual Legal Assistance Treaties (MLATs) to spur collaboration and data sharing. A sustainable effort requires a strategy and legal provisions to address international law, including data sharing and protection of privacy.

1. As we discussed, the Subcommittee is exploring possible legislation to address the botnet threat. What specific proposals would you recommend we include in such legislation?

   MLATs have been an effective mechanism to help enable the exchange of evidence and information in criminal and related matters for the past century. Recognizing the global scope of cybercrime, MLATs need to be overhauled. In addition, either supplemental or new MLATs between the United States and other counties which have become a safe-haven for cybercrime need to be explored. Related legislation including the Computer Fraud and Abuse Act (CFAA) need to be updated to include trafficking of access to botnets, perpetuating malvertising, click-fraud spam and related tactics. In the absence of such changes, criminals today can freely sell and trade access to botnets or execute denial-of-service (DDoS) attacks with little fear of legal ramifications.

2. Do you have any comments on the legislative proposals that Assistant Attorney General Caldwell discussed in her testimony?

   Faced with the evolving complexity of cybercrime and explosive explosive growth of cloud services, mobile devices and social media, OTA agrees with Assistant Attorney General Caldwell that the Computer Fraud and Abuse Act (CFAA) and the Electronic Communications Privacy Act (ECPA) are in need of updates. As the U.S. is becoming a data driven society and accumulating vast amounts sensitive data including location tracking, user profiling, bio-metrics and facial recognition data, we need to assure that such data should be afforded the same legal protections as documents and photos stored in your home or business. While individual data elements of these may appear benign, when combined they can be open for abuse. Search warrants based on probable cause need to be required before a service provider can be compelled to disclose a user's or businesses private communication or online documents.

3. How do we ensure that our laws give the public and private sectors the tools they need to respond to the botnet threat, while at the same time recognizing that the threat itself – and therefore the most effective responses to it – are constantly evolving?

   Updating ECPA and the CFAA and modernizing the MLAT process will help to create a legal environment that will allow the public and private sectors to work cooperatively to respond to botnets and related threats. Congress needs to help create incentives and remove barriers to information sharing while assuring privacy protections. Threat intelligence often contains personally identifiable information (PII), underscoring the importance that privacy be the foundation of all fraud prevention and data sharing practices. These privacy concerns can be easily addressed. When data is collected and used exclusively for threat detection, entities should be afforded "safe-harbor", providing that the data shared is not used or retained for any other purpose. Conversely, industry needs assurances that law enforcement will not use such data for purposes other than fighting cybercrime and to facilitate data sharing back to the private sector.

In summary, the public and private sector have a shared responsibility, including raising public awareness of the threats and promoting the adoption of best practices, standards and self-regulatory programs. With the right balance we can enhance online trust and confidence while promoting innovation. The Online Trust Alliance looks forward to working with the committee to develop balanced legislation, while promoting security and privacy enhancing best practices.

Sincerely,

Craig D. Spiezle

Craig D. Spiezle
Executive Director and President
Online Trust Alliance
Craigs@otalliance.org
+1 425-455-7400

RESPONSES OF PAUL VIXIE, PH.D., TO QUESTIONS SUBMITTED BY SENATOR WHITEHOUSE

August 4, 2014

The Honorable Patrick J. Leahy
Chairman
United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Mr. Chairman:

Thank you again for inviting me to testify at the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism hearing entitled "Taking Down Botnets: Public and Private Efforts to Disrupt and Dismantle Cybercriminal Networks" on July 15, 2014, and also for your letter of July 23 requesting additional written testimony. My answers (also representing the M^3AAWG position) to your written questions are as follows:

1. "As we discussed, the Subcommittee is exploring possible legislation to address the botnet threat. What specific proposals would you recommend we include in such legislation?"

First, I have a concern regarding the standards for *ex parte* injunctive relief when used as a tool for botnet takedowns. F.R.C.P. § 65(b)(1)(A) assumes that the court will be able to judge the clarity of the movant's claim of irreparable injury, loss, or damage. The Internet is a complex system, with an exquisite interdependence among its component parts, and the full framing of the issues at stake in a takedown provided by opposing technical experts will not (by definition) be explored at an *ex parte* proceeding. Effectively, the court currently has to take the movant's word for the clarity of their claims. I argue that a stronger standard is needed, noting that injunctive relief in support of a botnet takedown can have a wide-ranging impact on innocent third parties whose identities and Internet interdependencies literally cannot be foreseen by a movant.

Second, I note that in all botnet takedowns, private information belonging to affected parties, including botnet victims as well as third parties who are users of shared Internet components impacted by the takedown, may be placed into the hands of takedown operators. In any instance where a statutory duty or a specific contractual relationship such as employer-employee or provider-customer does not govern the handling of such information, the Subcommittee should ensure that a legal framework governing botnet takedowns appropriately balances the need to facilitate effective and expedient mitigation and remediation measures with the need to protect botnet victims and affected third parties against disclosure, retention, or use of such information.

2. "Do you have any comments on the legislative proposals that Assistant Attorney General Caldwell discussed in her testimony?"

Assistant Attorney General Caldwell's described amendments to the Computer Fraud and Abuse Act (CFAA) that would cover trafficking in access to botnets and would loosen the specification of a botmaster's intent; these are both well researched and they are borne out by my own recent experiences in the Internet security industry. Similarly, A.A.G. Caldwell's proposal to criminalize the overseas sale of stolen U.S. financial information will close a gaping loophole and help the letter of the law meet with its clear intent.

With regard to A.A.G. Caldwell's description of the DOJ's request for enhanced resources to combat botnets and other cyber threats, I am reminded of Attorney General Robert F. Kennedy's crusade against organized crime five decades ago. The United States is the richest target in the world for both individual and organized cybercrime and all of our lives are as affected by cybercrime today as we were by pre-cyber organized crime in 1960. We must do no less than RFK, and make the fight against this threat a top priority for our nation's law enforcement agencies. I support A.A.G. Caldwell's well-reasoned request for enhanced resources to combat botnets and other cyber threats and I expect that even more resources will be needed in the years ahead.

3. "How do we ensure that our laws give the public and private sectors the tools they need to respond to the botnet threat, while at the same time recognizing that the threat itself – and therefore the most effective responses to it – are constantly evolving?"

There is a bright middle ground where the best tradition of law exists: broad enough to accomplish our intended purposes, yet also narrow enough to resist misapplication, abuse, and overreach. Congress should strive for legislation to support the fight against botnets and cybercrime that first and foremost protects due process and individual rights, since any tradeoff of our nation's fundamental principles for temporary and targeted success against this or any threat would be a bad bargain. Within this envelope, I support the specific initiatives described by A.A.G. Caldwell in her testimony, noting that future wisdom as to cybercrime related legislative priorities is likely to come, as A.A.G. Caldwell's has come, from the women and men "in the trenches."

I would like to repeat my remark made during the July 15 subcommittee hearing: the Internet is borderless; the botnet problem is borderless; and any solution to the botnet problem will also be borderless. I also went on record describing the U.S. DOJ as the envy of the world in its approach to botnet takedowns and its awareness of the technical and social subtleties involved. The international law enforcement outreach and cooperation shown by the FBI and by the NCFTA perfectly demonstrates what I mean by "borderless solutions." We, the people of the United States, can only address this worldwide threat by efficiently and effectively cooperating with our peers around the world and by treating this as the world's problem, not merely a U.S. problem.

Mr. Chairman, thank you again for this opportunity to address your questions. I remain, as before, at your service.

Paul Vixie, CEO
Farsight Security, Inc.
August 4, 2014